Scientific Journal of Electronic & Cyber Defense
Vol. 12, No. 2, Summer 2024, Serial No. 46
ISSN: 2322-4347 , E-ISSN: 2980-8979

Image encryption using face biometric and metaheuristic algorithm over blockchain system

M.G. Hakemi [1], M.J. Rostami [2*]
Associate Professor, Shahid Bahonar University, Kerman, Iran .
(Received: 2024/04/27, Revised: 2024/07/19, Accepted: 2024/08/02, Published: 2024/08/23)
DOR:

ABSTRACT

With the expansion of the Internet network and public access to this network, the amount of information and data exchange increases day by day; Therefore, there will be a possibility of unauthorized access to the information that is exchanged. On the other hand, almost all programs that run on the Internet, such as social networks, have full access to images and content stored on the host device; Therefore, there is a possibility of unauthorized access and theft of personal information. Therefore, the security and accuracy of information must be guaranteed. In order to maintain the confidentiality of data, information encryption methods, such as image encryption algorithms, can be used. In the proposed method of this article, the encryption algorithm key is created with the help of information extracted from the person's face, image abstract, and public key so that the encryption algorithm will be highly sensitive to the change of any of the information used in key generation. Lorenz chaos mapping is used for image encryption in the substitution phase. Each color channel of the image is divided into four parts and each part is encrypted using a separate pseudo-random sequence and the encrypted image is produced. In the permutation phase, to achieve the best-encoded image, the genetic heuristic algorithm (GA) is used to bring the pixel correlation value of the encoded image to the minimum possible value by choosing the optimal parameters for the Arnold chaos mapping. According to the obtained results, the correlation values of pixels in all three horizontal, vertical, and diagonal directions are much smaller than other similar presented methods and the encryption algorithm has been able to significantly reduce the correlation and connection between pixels. Also, according to the results of NPCR and UACI differential analysis, it is higher than 99.6% and 33.4% for all the tested images, respectively. Therefore, the proposed method will have high resistance to statistical and differential attacks. Also, for the process of decoding the image, two-step authentication and safe storage of the encryption key are used in the blockchain network.

Keywords: Image encryption, Chaos, Genetic algorithm, Blockchain, Face detection, Authentication .

*Corresponding Author Email: rostami@uk.ac.ir

"پدافند الکترونیکی و سایبری"
سال دوازدهم، شماره ۲، تابستان ۱۴۰۳، ص ۸۳-۶۷

علمی – پژوهشی

رمزنگاری تصویر با استفاده از بیومتریک چهره و الگوریتم فراابتکاری بر روی سیستم زنجیره‌بلوکی

محمد گنجعلیخان حاکمی [۱]، محمدجواد رستمی [۲*]

۱- کارشناسی ارشد، ۲- استادیار، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه شهید باهنر کرمان، کرمان، ایران.

(دریافت: ۱۴۰۳/۰۲/۰۸، بازنگری: ۱۴۰۳/۰۳/۲۹، پذیرش: ۱۴۰۳/۰۵/۱۲، انتشار: ۱۴۰۳/۰۶/۱۳)

DOR:

ناشر: دانشگاه جامع امام حسین (ع) نویسندگان

چکیده

با گسترش شبکه اینترنت و دسترسی همگانی به این شبکه، میزان تبادل اطلاعات و داده‌ها روزبه‌روز افزایش می‌یابد؛ بنابراین، امکان دسترسی غیرمجاز به اطلاعاتی که مبادله می‌شوند وجود خواهد داشت. از طرفی تقریباً تمام برنامه‌هایی که بر بستر اینترنت اجرا می‌شوند، مانند شبکه-های اجتماعی، دسترسی کامل به تصاویر و محتوای ذخیره‌شده در دستگاه میزبان را دارا هستند؛ بنابراین امکان دسترسی غیرمجاز و سرقت اطلاعات شخصی وجود دارد. ازاین‌رو باید امنیت و صحت اطلاعات تضمین شود. به‌منظور حفظ محرمانگی داده‌ها می‌توان از روش‌های رمزنگاری اطلاعات، مانند الگوریتم‌های رمزنگاری تصویر استفاده کرد. در روش پیشنهادی این مقاله کلید الگوریتم رمزنگاری به کمک اطلاعات استخراج‌شده از چهره فرد، چکیده تصویر و کلید عمومی ایجاد می‌شود، بنابراین الگوریتم رمزنگاری نسبت به تغییر هر کدام از اطلاعات استفاده شده در تولید کلید حساسیت بالایی خواهد داشت. برای رمزنگاری تصویر در فاز جانشینی از نگاشت آشوب لورنز استفاده می‌شود. هر کانال رنگ تصویر به چهار قسمت تقسیم می‌شود و هر قسمت با استفاده از یک دنباله شبه‌تصادفی مجزا رمزنگاری می‌شود و تصویر رمز شده تولید می‌شود. در فاز جای‌گشت به‌منظور دست‌یافتن به بهترین تصویر رمز شده، از الگوریتم فراابتکاری ژنتیک (GA) استفاده می‌شود تا با انتخاب پارامترهای بهینه برای نگاشت آشوب آرنولد، مقدار همبستگی پیکسل‌های تصویر رمزنگاری شده به حداقل مقدار ممکن نزدیک شود. باتوجه‌به نتایج به‌دست‌آمده، مقادیر همبستگی پیکسل‌ها در هر سه جهت افقی، عمودی و قطری نسبت به سایر روش‌های ارائه شده مشابه بسیار کوچک‌تر است و الگوریتم رمزنگاری توانسته است به طور چشمگیری همبستگی و ارتباط بین پیکسل‌ها را کاهش دهد. همچنین باتوجه‌به نتایج تحلیل تفاضلی NPCR و UACI، برای تمام تصاویر آزمایش شده به ترتیب بالاتر از ۹۹/۶ درصد و ۳۳/۴ درصد است؛ بنابراین روش پیشنهادی دارای مقاومت بالایی نسبت به حملات آماری و تفاضلی خواهد داشت. همچنین برای فرآیند رمزگشایی تصویر، از احراز هویت دومرحله‌ای و نگهداری ایمن کلید رمزنگاری در شبکه زنجیره‌بلوکی استفاده می‌شود.

کلیدواژه‌ها: رمزنگاری تصویر، نگاشت آشوب، الگوریتم ژنتیک، احراز هویت، زنجیره‌بلوکی

۱- مقدمه

امروزه با گسترش شبکه‌های ارتباطی و اینترنت، حجم بسیار زیادی از اطلاعات در حال تولید و انتقال است که این امر منجر به اهمیت یافتن مسئلهٔ امنیت و صحت اطلاعات شده است. امنیت اطلاعات به معنی حفاظت اطلاعات، از فعالیت‌های غیرمجازی مانند دسترسی، استفاده، خواندن و یا تغییر اطلاعات است. برای حراست از اطلاعات، باید دسترسی به اطلاعات کنترل شود و فقط افراد مجاز باید توانایی دسترسی به اطلاعات را داشته باشند. به‌عنوان‌مثال از زمان ظهور شبکه‌های اجتماعی اولیه در اوایل سال ۲۰۰۰، شبکه‌های اجتماعی آنلاین به طور گسترده‌ای گسترش‌یافته‌اند که از معروف‌ترین این رسانه‌های اجتماعی در اواسط دهه ۲۰۱۰ فیس‌بوک[۲]، اینستاگرام[۳]، توییتر[۴] و اسنپ چت[۵] را می‌توان نام برد.

حجم عظیم اطلاعات شخصی که به‌صورت آنلاین در دسترس است و در فضای ابری ذخیره‌شده است، باعث شده که توانایی پایگاه‌داده‌ها در ذخیره‌سازی ایمن چنین اطلاعات شخصی کاهش

* رایانامه نویسنده مسئول: rostami@uk.ac.ir

[2] Facebook
[3] Instagram
[4] Twitter
[5] Snapchat

یابد و حفظ حریم خصوصی کاربران در اولویت قرار گیرد. آگاهی و مرزهای نقض حریم خصوصی، می‌تواند جز نگرانی‌های اساسی در عصر فنّاوری باشد [۱]. بخش بزرگی از داده‌های کاربران شامل تصاویر شخصی، مدارک مهم که به‌صورت فایل تصویری و یا متنی و... هستند که معمولاً در تلفن‌های همراه، رایانه‌های شخصی و دیسک‌های ذخیره‌سازی اطلاعات نگهداری می‌شوند. این نوع نگهداری از داده‌ها به دلایل زیادی می‌تواند خطرناک باشند ازجمله‌ی این دلایل می‌توان به هک شدن و یا ویروسی شدن دستگاه‌های نگهداری اطلاعات اشاره کرد؛ بنابراین استفاده از روش‌هایی که امنیت داده‌ها را نتیجه می‌دهند امری ضروری است.

یک از این روش‌ها رمزنگاری اطلاعات است [۲]. از مشهورترین و پرکاربردترین الگوریتم‌های رمزنگاری متقارن می‌توان به AES، DES، IDEA اشاره کرد. از مهم‌ترین الگوریتم‌های رمزنگاری کلید عمومی نیز می‌توان به RSA، ElGamal اشاره کرد که معمولاً برای داده‌هایی با ساختار متنی مورداستفاده قرار می‌گیرند؛ اما در رمزنگاری تصویر، به علت ساختار متفاوت تصاویر، که شامل وابستگی بالای اطلاعات پیکسل‌ها و اطلاعات آماری است، استفاده از روش‌های رمزنگاری متداول مناسب نخواهد بود [۳, ۴]. روش‌های مناسب برای تأمین امنیت تصاویر معمولاً در دودسته کلی قرار می‌گیرند: الف) پنهان کردن اطلاعات، که شامل پنهان نگاری[1] است، که در آن داده‌های مهم، درون داده‌های یک رسانه دیگر مثل تصویر یا ویدئو که رسانه پوششی[2] نام دارد پنهان می‌شود. بنابراین در ظاهر فقط یک تصویر یا ویدئو معمولی دیده می‌شود ولی در واقعیت اطلاعات مهمی در رسانه پوششی قرارگرفته شده است [۵]. ب) رمزنگاری[3]، که شامل تکنیک‌های آشوب، دنباله‌های DNA و... است [۶]. اغلب الگوریتم‌های رمزنگاری تصویر شامل دو مرحله اصلی هستند: مرحله جای‌گشت[4] و مرحله جانشینی[5]. در مرحله جای‌گشت فقط موقعیت پیکسل‌ها با یکدیگر جابجا می‌شوند و در مرحله جانشینی مقادیر پیکسل‌ها تغییر می‌کنند [۷]. پرکاربردترین تکنیک‌های استفاده‌شده در رمزنگاری تصویر شامل نگاشت‌های آشوب[6]، دنباله‌های DNA، چکیده تصویر و الگوریتم های فراابتکاری[7] است [۶]. نگاشت‌های آشوب جزء پرکاربردترین تکنیک‌ها در رمزنگاری تصویر هستند، که می‌توان در هر دو مرحله جانشینی و جای‌گشت از آن‌ها بهره برد [۸].

تانگ و همکارانش [۹] روشی به‌منظور افزایش سرعت و امنیت، رمزنگاری تصویر مبتنی بر سیستم آشوب ۴ بعدی ارائه دادند. در این روش نگاشت ۴ بعدی پیشنهادی، از ترکیب معادلات دو نگاشت سه‌بعدی لورنز[8] و چن[9] به دست می‌آید. به‌منظور رمزنگاری پیکسل‌های تصویر، ابتدا توسط نگاشت آشوب پیشنهادی، چهار دنباله آشوب تولید می‌شود. در این الگوریتم سعی می‌شود از دنباله‌های تولیدشده مجدد استفاده شود و به تعداد پیکسل‌های تصویر اعداد تصادفی دنباله تولید نشود؛ بنابراین تعدادی معین از اعداد دنباله‌ها انتخاب می‌شود و با قسمت ده‌دهی این اعداد سه کلید متفاوت ساخته می‌شود. در فاز جانشینی، تصویر به سه کانال رنگ تقسیم می‌شود و در مرحله اول سطرهای هر کانال رنگ با یک کلید متفاوت رمزنگاری می‌شوند. در مرحله دوم ستون‌های هر سه کانال رنگ با کلیدهای متفاوت از مرحله قبل رمزنگاری می‌شوند. همچنین در فاز جای‌گشت، از نگاشت آرنولد[10] برای درهم سازی موقعیت پیکسل‌ها استفاده می‌شود.

خلیل و همکارانش [۱۰] روشی برای رمزنگاری تصاویر رنگی یا خاکستری مطرح کردند. در این روش در هر دو فاز جانشینی و جای‌گشت از ترکیب نگاشت‌های آشوب استفاده‌شده است. ابتدا برای رمزنگاری تصویر رنگی، سه کانال رنگ تصویر جدا و تبدیل به یک بردار یک‌بعدی می‌شوند. در فاز جای‌گشت، از یک نگاشت دوبعدی پیشنهادشده sin-cosine استفاده می‌شود و یک دنباله شبه‌تصادفی با طول مشابه با بردار کانال رنگ تولید می‌شود. با فرض طول بردار N برای هر کانال رنگ، اعداد دنباله تصادفی به عددی بین ۰ تا N تبدیل می‌شوند و موقعیت هر پیکسل، متناظر با موقعیت جدیدش در دنباله تصادفی تغییر می‌کند. در فاز جانشینی از نگاشت یک‌بعدی ترکیب‌شده از دو نگاشت تنت[11] و لجستیک[12] استفاده می‌شود و دنباله‌ای هم طول با بردار پیکسل‌های درهم شده مرحله قبل ایجاد می‌شود و درنهایت با اعمال عملگر XOR تصویر رمز شده به دست می‌آید.

تنوع بالایی از نگاشت‌های آشوب وجود دارد که بر اساس ابعادشان و دنباله‌هایی که تولید می‌کنند در روش‌های مختلف مورداستفاده قرار می‌گیرند. به‌عنوان‌مثال، وانگ و همکارانش [۱۱] درروش پیشنهادی‌شان از یک نگاشت آشوب ۶ بعدی به همراه تکنیک دنباله‌های DNA استفاده کرده‌اند و یا درروش پیشنهادی ژو و همکارانش [۱۲] از چهار نگاشت آشوب متفاوت در فرآیند رمزنگاری استفاده‌شده است.

ژو و همکارانش [۱۳] روشی برای رمزنگاری تصاویر رنگی بر

[1] Steganography
[2] Cover-media
[3] Cryptography
[4] Permutation
[5] Substitution
[6] Chaotic functions
[7] Metaheuristic

[8] Lorenz system
[9] Chen system
[10] Arnold's cat map
[11] Tent map
[12] Logistic map

پایه مفهوم مربع لاتین و توابع آشوب معرفی کردند. در این روش ابتدا توسط نگاشت آشوب سه بعدی Sine، سه دنباله شبه‌تصادفی برای تولید مربع لاتین متعامد سه بعدی و ماتریس تطبیق تولید می‌شود. در مرحله دوم، تصویر اصلی توسط مربع لاتین ۳ بعدی و ماتریس منطبق جای‌گشت داده می‌شود. بدین صورت که هر صفحه از ماتریس جای‌گشت به شانزده قسمت تقسیم شده و شماره‌گذاری می‌شود. سپس، یک دنباله آشوب با ابعاد ۱ در ۱۶ باتوجه‌به سه دنباله از پیش تولید شده استخراج می‌شود. دنباله ۱۶تایی مرتب می‌شود و باتوجه‌به اندیس داریه‌ها قبل و بعد از مرتب سازی ۱۶ قسمت ماتریس جای‌گشت بایکدیگر جابجا می‌شوند. باتوجه‌به موقعیت جدید درایه‌های ماتریس جای‌گشت، تصویر اصلی درهم ریخته می‌شود و در آخرین مرحله با استفاده از شیفت چرخشی تصویر رمزنگاری تولید می‌شود.

ژانگ و همکارانش [۱۴] روشی مبتنی بر نگاشت آشوب و عملیات RNA ارائه دادند. این روش دارای سه مرحله اصلی است و در هر مرحله از دنباله‌های آشوب مجزایی استفاده می‌شود. بنابراین در اولین مرحله با استفاده از یک نگاشت آشوب ۶ بعدی به تعداد $(3 \times N \times N + 64) \times 6$ ماتریس آشوب ساخته می‌شود. از ماتریس‌های ساخته شده سه ماتریس S_1، S_2 و S_3 باتوجه‌به ابعاد موردنیاز در هر مرحله استخراج می‌شود. از ماتریس S_1 در اولین مرحله و به منظور جای‌گشت پیکسل‌ها استفاده می‌شود. ماتریس کانال رنگ و ماتریس S_1 به دو آرایه یک بعدی تبدیل می‌شوند. آرایه S_1 به صورت صعودی مرتب می‌شود و بر اساس اندیس‌ها قبل و بعد از مرتب سازی، درایه متناظر در آرایه کانال رنگ موقعیتش تغییر می‌کند. در مرحله دوم با استفاده از ماتریس S_2، مرحله جابه‌جایی انجام می‌شود. ماتریس کانال رنگ و ماتریس S_2 به صورت یک مکعب تغییر شکل می‌دهند. با استفاده از تکنیک زیگ‌زاگ که بر روی سه وجه مکعب انجام می‌شود پیکسل متناظر با درایه مکعب S_2 با استفاده از عملگر XOR رمز می‌شود. در آخرین مرحله پیکسل‌ها به صورت دودویی تبدیل می‌شوند و بر اساس بیت‌ها و چهار جدول کدون[1] RNA، پیکسل‌ها کدگذاری می‌شوند و تصویر رمز شده نهایی به دست می‌آید.

در روش‌های رمزنگاری تصویر که بر پایه چکیده تصویر هستند، ابتدا یک تابع چکیده ساز بر روی تصویر ورودی اعمال می‌شود و یک‌رشته خروجی با طول ثابت ایجاد می‌کند که از رشته تولیدشده می‌توان در مرحله پردازش کلید رمزنگاری، به‌دست‌آوردن مقادیر اولیه نگاشت آشوب و... استفاده کرد. طول ثابت رشته خروجی و حساس‌بودن خروجی به تغییر یک بیت در تصویر ورودی، از مزایای استفاده چکیده تصویر در رمزنگاری تصویر است [۱۵, ۱۶].

در روشی که توسط زارعی [۱۷] ارائه‌شده است از ترکیب دو تابع چکیده ساز MD5 و SHA-256 برای ساخت کلید ۲۵۶ بیتی رمزنگاری استفاده‌شده است. در این روش اطلاعات تصویر اصلی و یک کلید ۲۵۶ بیتی تصادفی با استفاده از توابع چکیده ساز درهم می‌شوند و یک کلید ۲۵۶ بیتی محرمانه را نتیجه می‌دهند که در فرآیند تولید دنباله‌های آشوب و رمزنگاری مورداستفاده قرار می‌گیرد.

ژانگ و همکارش [۱۸] روشی برای رمزنگاری تصاویر رنگی معرفی کردند. در این روش از چکیده تصویر، نگاشت‌های آشوب و دنباله‌های DNA استفاده شده است. در اولین مرحله برای تولید کلید، ابتدا چکیده تصویر اصلی محاسبه می‌شود. از چکیده تصویر در مقداردهی اولیه نگاشت‌های آشوب و تنظیم پارامترها استفاده می‌شود. برای تولید چکیده تصویر، ابتدا تصویر اصلی به یک تصویر سطح خاکستری تبدیل می‌شود. سپس یک ماتریس چکیده تصویر با ابعاد برابر با تصویر خاکستری ساخته می‌شود. هر دو ماتریس دارای ابعاد ۲۵۶ در ۲۵۶ هستند. درایه‌های ماتریس چکیده بدین صورت مقداردهی می‌شوند که اگر درایه $i+1$ ماتریس خاکستری از درایه i ام کوچکتر باشد، درایه متناظر در ماتریس چکیده مقدار ۱ قرار می‌گیرد، در غیر این صورت مقدار درایه صفر خواهد بود. سپس ماتریس چکیده به ابعاد ۴۰۹۶ در ۱۶ تغییر شکل می‌دهد. از ماتریس جدید ۱۶ مقدار به دست می‌آید که ۹ مقدار به صورت تصادفی انتخاب می‌شوند. در مرحله بعد که مرحله جای‌گشت است، تصویر به سه کانال رنگ مجزا تقسیم می‌شود. با استفاده از یک نگاشت آشوب دوبعدی و مقادیر به دست آمده از مرحله قبل، به ازای هر کانال رنگ دو دنباله شبه‌تصادفی X و Y ساخته می‌شود. هر دو دنباله به صورت صعودی مرتب می‌شوند و بر اساس اندیس دنباله، قبل و بعد از مرتب سازی سطرها و ستون‌های کانال‌های رنگ جای‌گشت داده می‌شوند.

در آخرین مرحله یعنی جابه‌جایی، ۶ دنباله شبه‌تصادفی توسط یک نگاشت آشوب ۶ بعدی ساخته می‌شود. سه دنباله به طور تصادفی انتخاب می‌شوند و مقادیرشان به بازه ۰ تا ۲۵۵ نگاشت می‌شود. از دو دنباله دیگر برای انتخاب قانون کدگذاری DNA، و از دنباله آخر برای انتخاب نوع عملیات حسابی DNA استفاده می‌شود. در نهایت تصویر باتوجه‌به قوانین و عملگرهای انتخابی کدگذاری شده و تصویر رمز شده نهایی حاصل می‌شود.

ژو و همکارانش [۱۹] روشی به منظور رمزنگاری تصویر ارائه دادند که سعی شده است تا امنیت سیستم‌های رمزنگاری که از یک نگاشت آشوب استفاده می‌کنند بهبود ببخشد. در این روش از نگاشت آشوب یک‌بعدی لجستیک استفاده‌شده است و مقدار اولیه نگاشت با استفاده از چکیده تصویر که با الگوریتم SHA-512 به‌دست‌آمده است، محاسبه می‌شود. سپس با استفاده از

[1] Codons

دنباله شبه‌تصادفی تولیدشده و الگوریتم خوشه‌بندی K-mediods، مرحله جای‌گشت تصویر انجام می‌شود. در مرحله جانشینی، تصویر به‌هم‌ریخته مرحله قبل، با استفاده از دنباله شبه‌تصادفی و عملگر XOR رمزنگاری می‌شود.

الگوریتم‌های فراابتکاری، الگوریتم‌های تکرارشونده‌ای هستند که در هر مرحله باتوجه‌به اطلاعاتی که از وضعیت فعلی مسئله دریافت می‌کنند، قادر خواهند بود مؤلفه‌های هدف مسئله را بهبود ببخشند [۲۰]. از الگوریتم‌های فراابتکاری به دلیل ماهیتشان در بهینه‌سازی، می‌توان در بهبود عملکرد فرآیند رمزنگاری استفاده کرد [۲۱, ۲۲].

عبدالله و همکارانش [۲۳] روشی برای رمزنگاری تصویر مطرح کردند که برای اولین بار از الگوریتم ژنتیک[1] در رمزنگاری تصویر استفاده شد. برای مقداردهی اولیه جمعیت ابتدا تصویر به چهار قسمت تقسیم می‌شود. سپس از نگاشت آشوب لجستیک برای رمزنگاری پیکسل‌های هر قسمت استفاده می‌شود. پس از رمزنگاری تصویر الگوریتم ژنتیک اعمال می‌شود تا درنهایت بهترین تصویر رمز شده انتخاب گردد. به این منظور از عملگر همبری[2] استفاده می‌شود و قسمت‌های تصویر با یکدیگر جابجا می‌شوند تا شرط تابع هدف[3] مسئله که کمینه کردن همبستگی[4] بین پیکسل‌ها است برآورده شود.

ژانگ و همکارانش [۲۴] روشی بر پایه سیستم آشوب 2DNLCML[5] و عملگرهای الگوریتم ژنیتک برای رمزنگاری تصاویر رنگی ارائه دادند. ابتدا مقادیر اولیه سیستم 2DNLCML، توسط نگاشت آشوب لجستیک تولید می‌شود. سپس سیستم 2DNLCML به اندازه ابعاد تصویر یعنی $M \times N$ تکرار می‌شود تا دنباله شبه‌تصادفی ساخته شود. در ادامه کانال‌های رنگ تصویر اصلی جدا می‌شوند و هر کانال رنگ به یک آرایه یک بعدی تبدیل می‌شود.

در مرحله بعد پیکسل‌های هر کانال با استفاده دنباله شبه‌تصادفی و عملگر XOR رمزنگاری می‌شود. در مرحله بعد باتوجه‌به مقدار درایه دنباله آشوب متناظر با پیکسلی که در مرحله قبل رمز شده است، عملیات جهش انجام می‌شود. بدین صورت که اگر مقدار درایه دنباله آشوب زوج باشد جهش Inversion، و اگر فرد باشد جهش Swap بر روی پیکسل اعمال می‌شود.

در آخرین مرحله عملیات همبری دونقطه‌ای انجام می‌شود. به این صورت که همبری ابتدا برای پیکسل‌های جفت کانال‌های قرمز و سبز، و بعد از آن برای جفت کانال‌های آبی و قرمز اعمال می‌شود. نقاط همبری با استفاده از مقادیر دنباله آشوب تولید شده، انتخاب می‌شوند. بسته به تعداد دورهای موردنیاز برای الگوریتم رمزنگاری مراحل ذکر شده تکرار می‌شوند و تصویر رمز شده حاصل می‌شود.

چای و همکارانش [۲۵] روشی ترکیبی بر پایه عملگرهای الگوریتم ژنتیک، ماتریس تنسور، نگاشت آشوب و دنباله‌های DNA به منظور رمزنگاری تصویر ارائه دادند. ابتدا توسط یک نگاشت آشوب ۶ بعدی، شش دنباله شبه‌تصادفی ساخته می‌شود. دو دنباله‌ی دیگر یعنی دنباله هفتم و هشتم با استفاده از شش دنباله قبل و عملگرهای جمع و تفریق تولید می‌شوند. از هشت دنباله تولید شده در مراحل مختلف رمزنگاری استفاده می‌شود.

در ادامه، تصویر اصلی به اجزای قرمز، سبز و آبی خود تقسیم می‌شود و هر کانال رنگ به چهار قسمت مساوی تقسیم می‌شود. یک ماتریس با استفاده از مقادیر یکی از هشت دنباله که به‌صورت تصادفی انتخاب می‌شود، ساخته می‌شود. اولین بلاک تصویر با استفاده از عملیات ضرب تنسور در ماتریس ساخته شده، ضرب می‌شود. بلاک جدید به‌صورت ساعت‌گرد با دیگر بلاک‌ها XOR می‌شود و کانال رنگ رمز شده حاصل می‌شود.

عملیات XOR بین دو کانال رنگ دیگر نیز انجام می‌شود تا سه کانال رنگ رمز شده حاصل شود. سپس با استفاده از اولین و دومین دنباله شبه‌تصادفی و قوانین کدگذاری DNA، تصویر کدگذاری می‌شود. در ادامه عملیات همبری و جهش به ترتیب توسط دنباله‌های سوم تا پنجم و ششم تا هشتم انجام می‌شود.

در نهایت کدگشایی DNA انجام می‌شود و تصویر رمز شده نهایی به دست می‌آید. انتخاب پارامترهای همبری ژنتیکی، تعیین نقاط تقاطع، موقعیت و قاعده جهش توسط اطلاعات تصویر اصلی و توالی‌های آشوبی کنترل می‌شوند. البته انجام عملیات ضرب تنسورها وقت‌گیر خواهد بود، بنابراین ممکن است روش ارائه شده برای کاربردهای بلادرنگ مناسب نباشد.

سعید خان و همکاران [۲۶] روشی مطرح کردند که در آن از الگوریتم PSO[6] به‌منظور ساخت یک S-Box با خاصیت غیرخطی بودن استفاده کردند. برای ساخت S-Box، ابتدا جمعیت اولیه الگوریتم PSO به‌صورت تصادفی مقداردهی می‌شود. سپس در هر مرحله با استفاده از موقعیت عامل‌های الگوریتم PSO یک S-Box ساخته می‌شود و توسط معیارهایی که غیرخطی بودن را بررسی می‌کنند ارزیابی می‌شود. درنهایت S-Box که خاصیت غیرخطی بالایی دارد انتخاب، و در مرحله جای‌گشت استفاده می‌شود.

همان‌طور که اشاره شد، برای تأمین امنیت داده‌ها استفاده از الگوریتم‌های رمزنگاری امری اجتناب‌ناپذیر است، اما مدیریت

[1] Genetic algorithm
[2] Crossover
[3] Fitness function
[4] Correlation
[5] Two Dimensional Nonlinear Coupled Map Lattices
[6] Particle swarm optimization

کلید رمزنگاری مسئله‌ای جدی و مهم است. در اکثر روش‌های ارائه‌شده در رمزنگاری تصویر، کلید رمزنگاری با استفاده از پارامترهای نگاشت آشوب، اطلاعات تصویر و... تولید می‌شود. برای افزایش امنیت رمزنگاری، می‌توان از مؤلفه‌های بیومتریک[1] در تولید کلید استفاده کرد و جهت ذخیره‌سازی ایمن کلید می‌توان از زنجیره‌بلوکی[2] بهره گرفت.

ژاو و همکارانش [۲۷] روشی برای رمزنگاری تصویر و احراز هویت[3] و صحت فرد فرستنده (رمزنگار) و گیرنده بر بستر زنجیره‌بلوکی معرفی کردند. در شبکه زنجیره‌بلوکی طراحی‌شده به هر کاربر (فرستنده یا گیرنده) یک شناسه منحصربه‌فرد که کلید عمومی است تعلق می‌گیرد. هر تراکنش شبکه زنجیره‌بلوکی شامل یک امضا خاص است که از چکیده تصویر رمز شده، کلید عمومی فرستنده، کلید عمومی گیرنده و کلید رمزنگاری با استفاده از الگوریتم SHA-256 حاصل می‌شود. در این سیستم فرستنده تصویر رمز شده را به همراه امضا بر روی شبکه ارسال می‌کند و پس از تأیید تراکنش توسط گره‌های شبکه، گیرنده می‌تواند درخواست خود را برای دریافت تصویر رمز شده ارسال کند و پس از احراز هویت و دریافت اطلاعات موردنیاز، رمزگشایی را انجام دهد.

لی و همکارانش [۲۸] یک روش رمزنگاری تصویر مبتنی برنگاشت آشوب و اثرانگشت بر بستر زنجیره‌بلوکی را ارائه کردند. در این روش کلید رمزنگاری با استفاده از اطلاعات اثرانگشت به دست می‌آید. همچنین اطلاعات اثرانگشت در تصویر رمزنگاری شده ثبت‌شده و انتقال تصاویر بین فرستنده و گیرنده بر بستر زنجیره‌بلوکی انجام می‌شود؛ بنابراین می‌توان از صحت هویت فرستنده و گیرنده اطمینان حاصل کرد.

در ادامه ساختار مقاله بدین صورت خواهد بود که در بخش دوم الگوریتم ژنتیک، توابع آشوب آرنولد و لورنز معرفی می‌شوند. سپس روشی که به‌منظور شناسایی و کدگذاری چهره استفاده شده است بررسی می‌شود. در بخش سوم، روش پیشنهادی با دید پایین‌به‌بالا شرح داده می‌شود. بدین معنا که ابتدا قسمت‌های جزئی سیستم بررسی می‌شود و سپس یک سیستم کامل برای رمزنگاری تصویر ارائه می‌شود. در بخش چهارم ابتدا معیارهای سنجش یک الگوریتم رمزنگاری تصویر معرفی می‌شوند و سپس با استفاده از جداول، نمودارها و تصاویر نتایج الگوریتم پیشنهادی بررسی می‌شود. همچنین نتایج روش پیشنهادی با سایر روش‌های ارائه شده مشابه مقایسه می‌شود تا کارایی الگوریتم پیشنهادی بررسی شود. در بخش پنجم نتیجه‌گیری تحقیق انجام شده بیان شده است.

۲- ۲- مفاهیم مقدماتی

در این بخش تکنیک‌ها و الگوریتم‌های استفاده‌شده درروش پیشنهادی معرفی می‌شوند. این بخش شامل معرفی نگاشت‌های آشوب لورنز و آرنولد، الگوریتم فراابتکاری ژنتیک و الگوریتم استخراج ویژگی‌های چهره است.

۲-۱- ۲-۱ نگاشت آشوب

نظریه آشوب شاخه‌ای از ریاضیات است که به بررسی رفتار آن دسته از سیستم‌های دینامیکی غیرخطی می‌پردازد که به شرایط اولیه بسیار حساس هستند [۲۹].

دنباله اعداد تولیدشده توسط نگاشت‌های آشوب در ظاهر تصادفی و بدون نظم و ترتیب هستند؛ اما در عمل وابسته به قوانین، الگوهای خاص و شرایط اولیه سیستم هستند. تاکنون نگاشت‌های آشوب متنوعی مانند لجستیک، استاندارد، آرنولد، هنون[4]، لورنز و... ارائه‌شده‌اند که هرکدام باتوجه‌به مؤلفه‌هایی مانند ابعاد نگاشت آشوب، تعداد پارامترها و رفتاری که نگاشت آشوب از خود نشان می‌دهد در کاربردهای مختلف استفاده می‌شوند.

۲-۲- ۲-۲ نگاشت آرنولد

نگاشت آرنولد در سال ۱۹۶۰ توسط ولادیمر آرنولد[5] معرفی شد. نگاشت آرنولد یک نگاشت دوبعدی است که طبق رابطه (۱) تعریف می‌شود [۳۰].

$$C = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \det C = 1$$
$$\begin{bmatrix} x' \\ y' \end{bmatrix} = C \begin{bmatrix} x \\ y \end{bmatrix} mod\ 1 \quad (۱)$$

که x و y موقعیت فعلی یک نقطه، x' و y' موقعیت جدید نقطه در فضای دوبعدی را نشان می‌دهند. و C یک ماتریس وارون‌پذیر است.

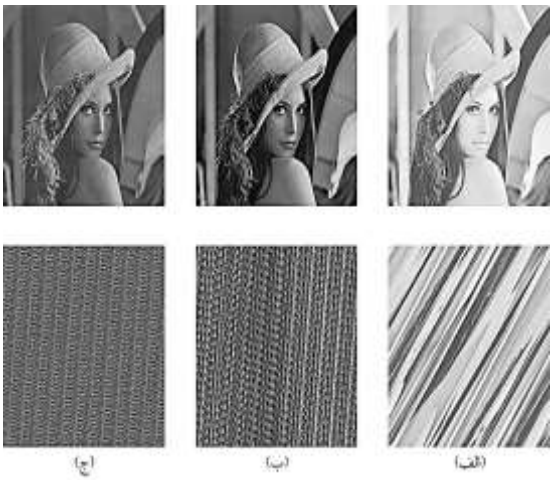
در فرآیند رمزنگاری تصویر می‌توان از نگاشت آرنولد به‌منظور به‌هم‌ریختن موقعیت پیکسل‌های تصویر استفاده کرد. برای این منظور، ابتدا ماتریس ثابت C در رابطه (۱) به شکل ماتریس C در رابطه (۲) به دلیل افزایش ضریب امنیت و خاصیت تصادفی بودن بازنویسی می‌شود که با اعمال این رابطه بر روی ماتریس دوبعدی تصویر، موقعیت پیکسل‌ها تغییر می‌کند [۳۱].

$$C = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}; \det C = 1;\ p, q \geq 0$$
$$\begin{bmatrix} x' \\ y' \end{bmatrix} = C \begin{bmatrix} x \\ y \end{bmatrix} mod\ N \quad (۲)$$

[1] Biometrics
[2] Blockchain
[3] Authentication
[4] Hénon map
[5] Vladimir Arnold

که x و y موقعیت فعلی یک پیکسل، x' و y' موقعیت جدید پیکسل در ماتریس دوبعدی تصویر و N ابعاد تصویر (با فرض مربعی بودن تصویر) را نشان می‌دهند.

به‌عنوان‌مثال، سه کانال رنگ آبی، سبز و قرمز تصویر لنا جداسازی شده و پیکسل‌های هر سه کانال رنگ به‌ازای پارامترهای مختلف جابه‌جا شده‌اند. برای کانال آبی پارامترهای $p = 12$ و $q = 71$ برای کانال سبز پارامترهای $p = 10$ و $q = 3$ و کانال قرمز پارامترهای $p = 1$ و $q = 2$ استفاده‌شده است. نتایج جابه‌جایی پیکسل‌های هر سه کانال رنگ در شکل (۱) نشان داده‌شده است.



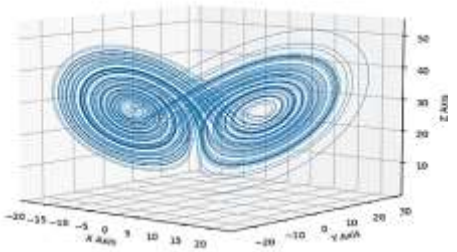
شکل (۱). اعمال نگاشت آشوب آرنولد بر روی سه کانال رنگ تصویر لنا. الف: کانال رنگ قرمز به ازای پارامترهای $p = 1$ و $q = 2$. ب: کانال رنگ سبز به ازای پارامترهای $p = 10$ و $q = 3$. ج: کانال رنگ آبی به ازای پارامترهای $p = 12$ و $q = 71$.

۲-۳- ۲-۳ نگاشت لورنز

سیستم لورنز یک سیستم دیفرانسیل معمولی، غیرخطی و سه‌بعدی است که در سال ۱۹۶۳ توسط ادوارد لورنز[1] به‌منظور مدل‌سازی ریاضی همرفت جوی معرفی شد [۳۲]. سیستم لورنز استاندارد، دارای سه پارامتر σ، ρ و β هستند که به‌صورت رابطه (۳) معرفی می‌شود.

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \quad (۳)$$

که σ، ρ و β مقادیر مثبت هستند که به ترتیب به ازای مقادیر ۱۰، ۲۸ و $\frac{۸}{۳}$ سیستم رفتار آشوبناک نشان خواهد داد. $x_0 = 0.27$، $y_0 = 1.0$ و $z_0 = 0.63$ توابعی برحسب زمان هستند که مقادیر جدید را بر اساس مقادیر قبلی دنباله تولید می‌کنند. در شکل (۲) مثالی از رفتار سیستم لورنز به ازای مقادیر اولیه $x_0 = 0.27$، $y_0 = 1.0$ و $z_0 = 0.63$ و پارامترهای ذکرشده در ۱۰۰۰۰ تکرار نشان داده‌شده است.



شکل (۲). مثالی از رفتار نگاشت آشوب لورنز به ازای مقادیر اولیه $x_0 = 0.27$، $y_0 = 1.0$ و $z_0 = 0.63$ و پارامترهای $\sigma = 10$، $\rho = 28$ و $\beta = \frac{8}{3}$

۲-۴- ۲-۴ الگوریتم ژنتیک

الگوریتم ژنتیک، یک روش جستجو و بهینه‌سازی بر اساس اصول تکامل طبیعی است [۳۳]. این الگوریتم جزء الگوریتم‌های تکاملی قرار می‌گیرد که بر اساس تئوری تکامل انتخاب طبیعی داروین پایه‌گذاری شده است. در این الگوریتم‌ها، یک جمعیت از طریق انتخاب اعضای برتر و کنار گذاشتن اعضای پست‌تر در طی فرآیند تولیدمثل و تکامل، بهبود می‌یابد. الگوریتم ژنتیک اجازه می‌دهد که یک جمعیت متشکل از تعداد زیادی افراد که تحت قوانین ویژه‌ای تشکیل‌شده‌اند، در طی فرآیند تکامل تابع هدف را بهینه نمایند. الگوریتم ژنتیک با ایجاد یک جمعیت اولیه از کروموزوم‌ها[2] آغاز می‌شود. به‌عبارتی‌دیگر کروموزوم‌ها، رشته‌هایی از مقادیر پیشنهادی برای متغیرهای تصمیم مسئله هستند و هر یک نمایانگر یک پاسخ محتمل برای مسئله هستند. در مرحله بعد، کروموزوم‌ها باتوجه‌به هدف بهینه‌سازی مورد ارزیابی قرار می‌گیرند و کروموزوم‌هایی که پاسخ‌های بهتری برای مسئله موردنظر محسوب می‌شوند، شانس بیشتری برای تولید مجدد جواب‌های مسئله پیدا می‌کنند.

در مرحله تولیدمثل سه عملگر مهم و کلیدی وجود دارد: ۱) عملگر انتخاب: با استفاده از این عملگر از بین کروموزوم‌های موجود در جمعیت تعدادی برای تولیدمثل انتخاب می‌شوند. انتخاب کروموزوم‌ها به‌صورت تصادفی اتفاق می‌افتد اما باید به‌گونه‌ای باشد که کروموزوم‌هایی که شایستگی بیشتر دارند، احتمال بیشتری برای انتخاب داشته باشند. ۲) عملگر همبری: این عملگر بر روی دو یا چند والد اعمال می‌شود و با ادغام و یا تعویض برخی از ژن‌ها دو یا چند فرزند تولید می‌شود. ۳) عملگر جهش[3]: این عملگر یک یا چند ژن را به‌صورت تصادفی تغییر می‌دهد.

۲-۵- ۲-۵ استخراج ویژگی‌های چهره

[1] Edward Norton Lorenz

[2] Chromosome
[3] Mutation

استفاده از ویژگی‌های بیومتریک در فرآیند تولید کلید و احراز هویت اولین‌بار در سال ۱۹۹۴ مطرح شد [۳۴]. در این‌گونه روش‌ها می‌توان از ویژگی‌هایی مانند چهره، اثرانگشت، قرنیه، صوت و ... استفاده کرد که به دلیل منحصربه‌فرد بودن اطلاعات نسبت به سایر افراد، و عدم نیاز به نگهداری امن این ویژگی‌ها در بسیاری از کاربردهای رمزنگاری و احراز هویت استفاده می‌شوند [۳۵]. ویژگی‌های چهره یک فرد شامل اطلاعاتی است که در قالب برداری با مقادیر عددی شناخته می‌شود. هرکدام از مقادیر این بردار یک ویژگی را بیان می‌کند، مانند فاصله بین دو چشم، طول ابرو، فاصله بین لب تا چانه و... که برای هر فرد منحصربه‌فرد خواهد بود. استخراج ویژگی‌های چهره به‌صورت کلی در دو مرحله انجام می‌شود [۳۶]: ۱) شناسایی چهره[1] ۲) کدگذاری چهره[2].

۱) شناسایی چهره: در این مرحله قسمتی از تصویر که چهره فرد را شامل می‌شود شناسایی می‌شود که می‌توان از الگوریتم‌های متنوعی مانند HOG، MTCNN و SVM استفاده کرد [۳۷–۳۹].

۲) کدگذاری چهره: به‌منظور کدگذاری چهره می‌توان از شبکه‌های عصبی کانولوشن[3] استفاده کرد. شبکه FaceNet در سال ۲۰۱۵ توسط محققان گوگل معرفی شد [۴۰]. آموزش این شبکه بر روی‌داده‌های LFW[4] انجام‌شده و دقت تشخیص این مدل ۹۹/۶۳ درصد است. این روش به دلیل دقت بالاتر نسبت به روش‌هایی مانند VGG-Face و DeepID که به ترتیب دارای ۹۷/۷۸ و ۹۹/۱۵ درصد هستند در کاربردهای بیشتری استفاده می‌شود. خروجی این شبکه یک بردار عددی ۱۲۸ تایی است که هر مؤلفه از آن نشان‌دهنده‌ی یک ویژگی چهره است.

۳- ۳- روش پیشنهادی

در این بخش روش پیشنهادی رمزنگاری تصویر بیان می‌شود. کلید رمزنگاری با استفاده از اطلاعات چهره کاربر، کلید عمومی و تصویر اصلی ساخته می‌شود. در فاز جانشینی پیکسل‌ها هر قسمت از تصویر با استفاده از یک دنباله شبه‌تصادفی جداگانه رمزنگاری می‌شود. در فاز جای‌گشت، به‌وسیلهٔ الگوریتم ژنتیک یک حالت بهینه برای به‌هم‌ریختن پیکسل‌ها انتخاب می‌شود تا همبستگی بین پیکسل‌ها به طور مناسبی کاهش یابد.

۳-۱- ۳-۱ چکیده تصویر

محاسبه چکیده تصویر به‌وسیلهٔ الگوریتم SHA-512 انجام می‌شود. برای محاسبه چکیده تصویر، ابتدا مقادیر پیکسل‌های هر سه کانال رنگ (در تصاویر خاکستری یک کانال رنگ) به رشته‌ای از بایت‌ها تبدیل می‌شود و به‌عنوان ورودی به تابع محاسبه چکیده اعمال می‌شود و یک خروجی ۵۱۲ بیتی که متأثر از تمام پیکسل‌های تصویر است را نتیجه می‌دهد.

۳-۲- ۳-۲ کلید عمومی و خصوصی

از جفت کلیدهای عمومی و خصوصی در فرآیند رمزگشایی و احراز هویت استفاده می‌شود. درروش پیشنهادی از کلیدهای ۱۰۲۴ بیتی که توسط الگوریتم RSA تولید می‌شوند استفاده می‌شود.

۳-۳- ۳-۳ بردار ویژگی‌های چهره

اطلاعات چهره فرد رمزگذار با استفاده از الگوریتم‌های معرفی‌شده در بخش ۲-۵ استخراج و کدگذاری می‌شوند؛ و خروجی نهایی یک بردار است که دارای ۱۲۸ درایه اعشاری است و هر درایه نشان‌دهنده یک یا ترکیبی از چند ویژگی چهره مانند فاصله دو چشم، طول لب‌ها و... است.

۳-۴- ۳-۴ مقادیر اولیه نگاشت لورنز

همان‌طور که در بخش ۲-۳ نگاشت لورنز بررسی شد، این نگاشت به سه مقدار اولیه نیاز خواهد داشت. درروش پیشنهادی ابتدا تصویر همانند شکل (۳) به چهار قسمت تقسیم می‌شود سپس به ازای هر قسمت سه دنباله آشوب برای رمزنگاری سه کانال رنگ تولید می‌شود؛ بنابراین به ۱۲ دنباله آشوب نیاز است که به این منظور باید ۱۲ مقدار اولیه مشخص شوند.

برای تولید مقادیر اولیه نگاشت، ابتدا توسط الگوریتم SHA-512 چکیده سه داده، چکیده تصویر، بردار ویژگی‌های چهره و کلید عمومی محاسبه می‌شود. رشته ۵۱۲ بیتی نهایی به چهار قسمت مساوی ۱۲۸ بیتی تقسیم می‌شود. در مرحله بعد هر قسمت ۱۲۸ بیتی به سه رشته ۴۰ بیتی تقسیم می‌شود. در اینجا از ۸ بیت کم ارزش هر کدام از رشته‌های ۱۲۸ بیتی صرف نظر می‌شود. سپس بیت‌های هرکدام از رشته‌های ۴۰ بیتی دوبه‌دو (بیت‌های مجاور) با یکدیگر XOR می‌شوند. در آخرین مرحله سه بردار ۳۹ بیتی دودویی به سه عدد ده‌دهی تبدیل می‌شوند.

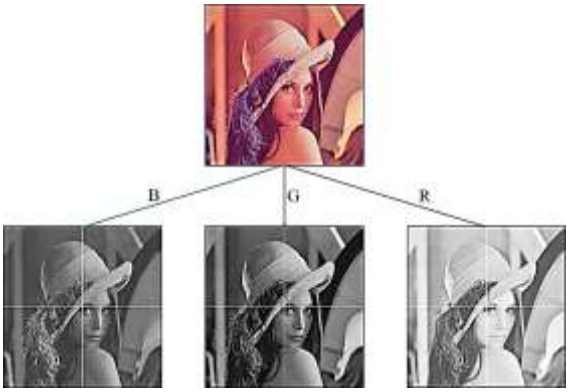
سه عدد به‌دست‌آمده طبق رابطه (۴) به سه عدد بین ۰ و ۱ تبدیل خواهند شد. با تکرار مراحل ذکرشده برای ۴ قسمت تصویر و هر سه کانال رنگ، ۱۲ مقدار اولیه بین ۰ و ۱ برای نگاشت آشوب لورنز به دست می‌آید.

$$x_i, y_i, z_i = \frac{b2d(\vec{x}) \,\%\, 2^8}{2^8} \qquad (۴)$$

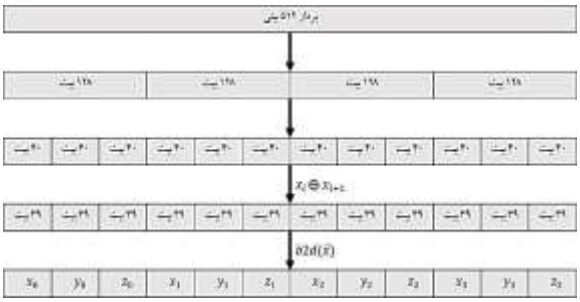
که در رابطه (۴)، $\vec{x}$ بردار ۳۹ بیتی، $b2d()$ تابعی برای تبدیل عدد دودویی به عددی ده‌دهی و $\%$ عملگر محاسبه باقی‌مانده تقسیم است؛ بنابراین مقادیر اولیه نگاشت متأثر از کلید عمومی، ویژگی‌های چهره و مقادیر پیکسل‌های هر سه کانال رنگ

[1] Face detection
[2] Face encoding
[3] Convolutional neural network
[4] Labeled Faces in the Wild

خواهد بود. مراحل محاسبه مقادیر اولیه نگاشت آشوب در شکل (۴) نشان داده‌شده است.



شکل (۳). جداسازی کانال‌های رنگ تصویر لنا و تقسیم‌بندی هر کانال رنگ به چهار قسمت مساوی



شکل (۴). مراحل محاسبه دوازده مقدار اولیه برای نگاشت آشوب لورنز

۳-۵- ۵-۳ تولید دنباله‌های شبه‌تصادفی

با استفاده از ۱۲ مقدار اولیه تولیدشده در بخش ۳-۴، ۱۲ دنباله شبه‌تصادفی تولید می‌شود. برای تولید دنباله از نگاشت آشوب لورنز با پارامترهای معرفی‌شده در بخش ۲-۳ استفاده می‌شود. ابتدا سه دنباله S_{01}، S_{02} و S_{03} با استفاده از سه مقدار اولیه x_0، y_0 و z_0 تولید می‌شوند. سپس سه دنباله S_{11}، S_{12} و S_{13} با استفاده از سه مقدار اولیه x_1، y_1 و z_1 تولید می‌شوند. به طور مشابه طبق رابطه (۵)، دوازده دنباله شبه‌تصادفی تولید می‌شوند.

$$\begin{aligned} S_{01}, S_{02}, S_{03} &= Lorenz\_System(x_0, y_0, z_0) \\ S_{11}, S_{12}, S_{13} &= Lorenz\_System(x_1, y_1, z_1) \\ S_{21}, S_{22}, S_{23} &= Lorenz\_System(x_2, y_2, z_2) \\ S_{31}, S_{32}, S_{33} &= Lorenz\_System(x_3, y_3, z_3) \end{aligned} \quad (۵)$$

که در رابطه (۵)، $Lorenz\_System(x_i, y_i, z_i)$ تابعی است برای تولید سه دنباله شبه‌تصادفی با استفاده سه مقدار اولیه ورودی و S_{ij} j امین دنباله تولیدشده با استفاده از i امین دسته مقادیر اولیه است. درروش پیشنهادی طول دنباله‌های تولیدشده با یکدیگر برابر، و برابر با تعداد پیکسل‌های یکی از چهار قسمت تصویر است بنابراین اگر تصویر اصلی N سطر و M ستون داشته باشد و چهار قسمت مساوی تقسیم شود، طول هر دنباله $M / 4 \times N / 4$ خواهد بود.

۳-۶- ۶-۳ الگوریتم رمزنگاری

الگوریتم رمزنگاری پیشنهادی دارای دوفاز اصلی جانشینی (تغییر مقادیر پیکسل‌ها) و جای‌گشت (تغییر موقعیت پیکسل‌ها) است که در شکل (۵) نشان داده‌شده است. همچنین الگوریتم رمزنگاری و رمزگشایی مشابه هستند و تنها در برخی از پارامترهای ورودی متفاوت هستند. درروش پیشنهادی هر کانال رنگ به طور جداگانه رمزنگاری می‌شود. الگوریتم رمزنگاری شامل ۴ مرحله زیر است:

مرحله اول: استخراج ویژگی‌های بیومتریک چهره و محاسبه چکیده تصویر.

مرحله دوم: محاسبه ۱۲ مقدار اولیه نگاشت آشوب لورنز.

مرحله سوم: در این مرحله فاز جانشینی پیکسل‌ها انجام می‌شود. هرکدام از کانال‌های رنگ به چهار قسمت تقسیم می‌شوند و هرکدام از قسمت‌ها، با استفاده از یکی از دنباله‌های S_{ij} تولیدشده در بخش ۳-۵ رمزنگاری می‌شوند. برای رمزنگاری سه حالت در نظر گرفته می‌شود. اگر کانال رنگ قرمز باشد قسمت‌های اول تا چهارم این کانال به ترتیب با استفاده از دنباله‌های S_{01}، S_{11}، S_{21} و S_{31} و اگر کانال رنگ سبز باشد قسمت‌های اول تا چهارم این کانال به ترتیب با استفاده از دنباله‌های S_{02}، S_{12}، S_{22} و S_{32} و اگر کانال رنگ آبی باشد قسمت‌های اول تا چهارم این کانال به ترتیب با استفاده از دنباله‌های S_{03}، S_{13}، S_{23} و S_{33} با استفاده از رابطه‌ی (۶) رمزنگاری می‌شوند.

$$Pix_{New} = [Pix_{Old} \oplus round\,(S_{ij} \times 255)]\%256 \quad (۶)$$

که Pix_{New} مقدار جدید پیکسل، Pix_{Old} مقدار فعلی پیکسل، S_{ij} دنباله شبه‌تصادفی، $round$ عبارت ورودی را به نزدیک‌ترین عدد صحیح تبدیل می‌کند، $\oplus$ علامت XOR و $\%$ علامت محاسبه باقی‌مانده است. بنابراین هر چهار قسمت کانال‌های رنگ رمزنگاری می‌شوند. سپس چهار قسمت هر کانال مجدد کنار یکدیگر قرار می‌گیرند.

مرحله چهارم: در این مرحله فاز جای‌گشت انجام می‌شود و موقعیت پیکسل‌های رمز شده کانال‌های رنگ به‌دست‌آمده از مرحله قبل توسط نگاشت آرنولد که در بخش ۲-۲ معرفی شد، به‌هم‌ریخته می‌شوند. دو پارامتر اصلی a و b در نگاشت آرنولد به‌صورت ثابت تنظیم نمی‌شوند، بلکه توسط الگوریتم فرابتکاری ژنتیک بهینه‌ترین پارامترها انتخاب می‌شوند. به‌منظور انتخاب بهینه پارامترهای نگاشت آرنولد توسط الگوریتم فرابتکاری ژنتیک مراحل زیر طی می‌شوند:

الف) مقداردهی اولیه عامل‌ها: در این مرحله جمعیت الگوریتم بهینه‌سازی را مقادیر مختلف پارامترهای a و b می‌سازند. بنابراین مسئله دارای دو متغیر است. هرکدام از متغیرها

یک عدد صحیح مثبت هستند که در اینجا مقدار هر متغیر در بازه‌ی [۱،۶۵۵۳۵] قرار می‌گیرد؛ یعنی برای هر متغیر ۱۶ بیت در نظر گرفته می‌شود. به‌عنوان‌مثال اگر جمعیت دارای ۱۰۰ عضو باشد و هر عضو دارای دو متغیر باشد، بنابراین یک ماتریس ۱۰۰ ✕ ۳۲ به‌صورت تصادفی ساخته می‌شود.

ب) ارزیابی عامل‌ها: پس از ساخت جمعیت اولیه نوبت به ارزیابی عامل‌ها است تا شایسته‌ترین عامل مشخص شود. برای ارزیابی عامل‌ها، تابع شایستگی؛ همبستگی بین پیکسل‌های تصویر تعریف می‌شود؛ یعنی به‌ازای متغیرهای a و b یک عامل، پیکسل‌های تصویر توسط نگاشت آرنولد به‌هم‌ریخته می‌شوند. سپس مقدار همبستگی پیکسل‌های سطر، ستون و قطر ماتریس به‌هم‌ریخته شده اندازه‌گیری می‌شود؛ بنابراین بهینه‌سازی بر روی سه هدف به طور هم‌زمان باید انجام شود. ازاین‌رو مسئله چند هدفِ را با استفاده از روش مجموع وزن‌دار اهداف، به یک مسئله تک هدفِ تبدیل می‌کنیم؛ بنابراین سه مقدار اندازه‌گیری شده با وزن‌های یکسان با یکدیگر جمع می‌شوند تا یک عدد صحیح را نتیجه دهند. عدد به‌دست‌آمده نشان‌دهنده شایستگی آن عامل خواهد بود و هر چه این مقدار کمتر باشد، شایستگی عامل بیشتر خواهد بود؛ بنابراین بهینه‌سازی مسئله، کمینه‌سازی تابع هدف است.

ج) بروز رسانی جمعیت: عامل‌ها بر اساس شایستگی‌شان به‌روزرسانی می‌شوند و جمعیت مرحله بعد ساخته می‌شود (انتخاب، همبری، جهش).

د) پاسخ نهایی: درنهایت پس از رسیدن به‌شرط توقف مسئله که در اینجا تعداد تکرارهای الگوریتم فراابتکاری تنظیم‌شده است، بهترین مقادیر a و b برای نگاشت آرنولد انتخاب می‌شوند و جای‌گشت تصویر انجام می‌شود.

شکل (۵). شماتیک الگوریتم رمزنگاری پیشنهادی که دارای دو فاز اصلی جانشینی و جایگشت است.

۳-۷- ۳-۷ کلید رمزنگاری

کلید رمزنگاری و رمزگشایی یکسان خواهند بود. همچنین کلید باید دارای طول قابل‌قبولی برای تأمین امنیت باشد. کلید با استفاده از اطلاعاتی که در رمزنگاری استفاده‌شده است ساخته می‌شود. ابتدا رشته ۵۱۲ بیتی حاصل از چکیده کلید عمومی، ویژگی‌های چهره و چکیده تصویر نیاز است. همچنین نگاشت لورنز دارای سه پارامتر اعشاری است بنابراین برای هر پارامتر ۶۴ بیت در نظر گرفته می‌شود که درمجموع ۱۹۲ بیت نیاز خواهد داشت. آخرین قسمت کلید شامل پارامترهای نگاشت آرنولد خواهد بود که در فاز جای‌گشت تصویر استفاده‌شده‌اند. برای هر متغیر به ۱۶ بیت نیاز است که درمجموع برای ۶ متغیر در تصاویر رنگی (۲ متغیر به ازای هر کانال رنگ) و ۲ متغیر در تصاویر خاکستری به ترتیب ۹۶ و ۳۲ بیت نیاز است؛ بنابراین در تصاویر رنگی طول کلید ۸۰۰ بیت و در تصاویر خاکستری ۷۳۶ بیت خواهد بود. ترتیب قرارگیری اطلاعات و ساخت کلید این‌گونه خواهد بود که ابتدا رشته ۵۱۲ بیتی در سمت چپ، پس‌ازآن رشته ۱۹۲ بیتی و در آخر رشته ۹۶ بیتی یا ۳۲ بیتی بسته به نوع تصویر کنار یکدیگر قرار می‌گیرند.

۳-۸- ۸-۳ ذخیره کلید در زنجیره‌بلوکی

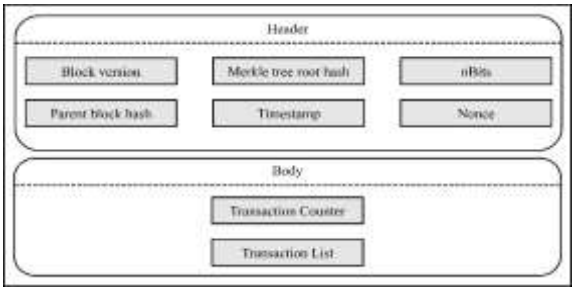
به‌منظور نگهداری ایمن کلید رمزنگاری و همچنین احراز هویت کاربر، پس از رمزنگاری تصویر، کلید تولیدشده در بخش ۳-۷ و بردار ویژگی‌های چهره کاربر در یک شبکه زنجیره‌بلوکی ذخیره‌سازی می‌شوند. در شبیه‌سازی زنجیره‌بلوکی روش پیشنهادی، از IPFS[1] مبتنی بر اتریوم[2] با استفاده از زبان برنامه‌نویسی Golang استفاده‌شده است. ساختار بلوک‌ها در شبکه در شکل (۶) نشان داده‌شده است. هر بلوک دارای دو قسمت اصلی تیتر[3] و بدنه[4] است. در قسمت تیتر؛ نسخه شبکه زنجیره‌بلوکی، مهر زمانی[5]، رشته Nonce، درجه سختی، چکیده بلوک قبل و ریشه درخت مرکل قرار می‌گیرد. در قسمت بدنه بلوک تراکنش‌ها قرار می‌گیرند، هر تراکنش به‌صورت رابطه (۷) تعریف می‌شود.

$$Transaction = Enc[(Face\ Vector, Key), Public\ Key] \quad (۷)$$

که $Enc[(x), Public\ Key]$ رمزنگاری داده x با استفاده

[1] InterPlanetary File System
[2] Ethereum
[3] Header
[4] Body
[5] Timestamp

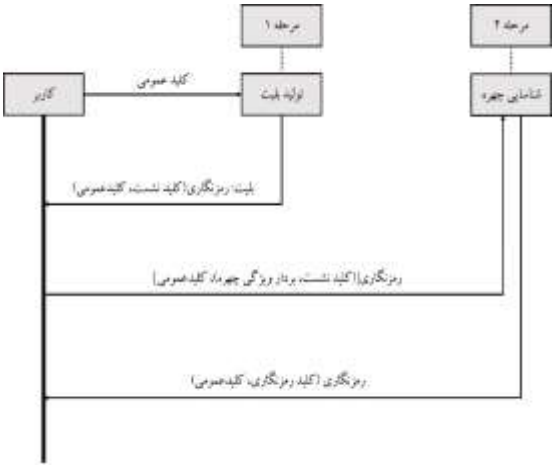
از الگوریتم RSA و کلید عمومی $Public\ Key$، بردار ویژگی‌های چهره و $Face\ Vector$ کلید Key ۸۰۰ بیتی (تصاویر رنگی) یا ۷۳۶ بیتی (تصاویر خاکستری) است.



شکل (۶). ساختار یک بلوک در زنجیره‌بلوکی

۳-۹- ۹-۳ رمزگشایی و احراز هویت

به‌منظور رمزگشایی تصاویر دو مرحله احراز هویت اجرا می‌شود. سیستم احراز هویت دومرحله‌ای روش پیشنهادی در شکل (۷) نشان‌داده‌شده است. در اولین مرحله کاربر برای رمزگشایی تصویر، کلید عمومی خود را به‌عنوان یک شناسه کاربری ارسال می‌کند. سیستم یک بلیت (پیام) که حاوی کلید موقت نشست است را با استفاده از کلید عمومی کاربر رمزنگاری و برای کاربر ارسال می‌کند. تنها، فردی می‌تواند به کلید نشست دسترسی پیدا کند که بتواند بلیت را با استفاده از کلید خصوصی‌اش رمزگشایی کند. همچنین ارائه بلیت برای رسیدن به مرحله دوم الزامی است. در مرحله دوم، تصویری از چهره فرد دریافت می‌شود. سپس بردار ویژگی‌های چهره استخراج می‌شود. ویژگی‌های چهرهٔ دریافتی با بردار ویژگی‌های چهره ذخیره‌شده در زنجیره‌بلوکی مطابق بخش ۳-۱۰ مطابقت داده می‌شوند. اگر تأیید شود که چهره فرد درخواست‌کننده با چهره فرد رمزنگار یکسان است (درخواست‌کننده همان فرد رمزگذار است) کلید موردنیاز رمزگشایی که در زنجیره‌بلوکی ذخیره‌شده است، برای کاربر ارسال می‌شود. پس از دریافت کلید رمزنگاری، فرآیند رمزگشایی معکوس رمزنگاری خواهد بود.



شکل (۷). احراز هویت دومرحله‌ای به‌منظور رمزگشایی تصویر

۳-۱۰- ۱۰-۳ تطابق چهره

به‌منظور مشخص‌کردن انطباق دو چهره کافی است که بردار ویژگی‌های دو چهره استخراج شوند. سپس فاصلهٔ بین دو بردار اندازه‌گیری شود. اگر فاصلهٔ بین دو بردار از یک حد آستانه بیشتر باشد انطباق دو چهره رد می‌شود؛ اما اگر فاصله از حد آستانه کمتر باشد، انطباق چهره‌ها تأیید می‌شود. برای اندازه‌گیری فاصله دو بردار از فاصله اقلیدسی استفاده می‌شود:

فاصله اقلیدسی: فاصله بردار ویژگی اول x و بردار ویژگی دوم y طبق رابطه (۸) محاسبه می‌شود.

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \qquad (۸)$$

که $i = 1,2,\dots,n$ اندیس ویژگی‌ها و n تعداد ویژگی‌ها است. مقادیر حد آستانه به‌صورت آزمایشی و تجربی به‌دست‌آمده‌اند که بسته به مدل یادگیری متفاوت هستند. مقادیر حد آستانه برای مدل FaceNet، برای فاصله‌های اقلیدسی و اقلیدسی نرمال شده، مقادیر ۱۰ و ۰/۸ هستند.

۴- ۴- ارزیابی و نتایج

برای بررسی عملکرد و کارایی یک الگوریتم رمزنگاری، نیاز است آزمایش‌هایی بر روی نتایج به‌دست‌آمده از آن الگوریتم صورت گیرد. در الگوریتم‌های رمزنگاری تصاویر، هدف اصلی آزمایش‌ها سنجش میزان امنیت الگوریتم و مقاومت در برابر انواع حملات است. در آزمایش‌های انجام‌شده از الگوریتم ژنتیک دودویی با اندازه جمعیت ۱۰۰ استفاده‌شده است. برای هر متغیر ۱۶ بیت در

نظر گرفته‌شده است.

روش‌های استفاده‌شده در مراحل مختلف الگوریتم ژنتیک به شرح زیر می‌باشد: ۱- عملگر انتخاب: انتخاب تورنمنت[1]؛ ۲- مقیاس‌کردن شایستگی: انتخاب بولتزمن[2]؛ ۳- عملگر همبری: غیریکنواخت مبتنی بر ماسک الگو. ۴- تعداد تکرارها: ۳۰ تکرار. همچنین در تمام آزمایش‌ها نرخ جهش و همبری به ترتیب برابر با ۰/۰۵ و ۰/۹ است.

۴-۱- ۱-۴ تحلیل تفاضلی

تحلیل تفاضلی بر پایه میزان حساس‌بودن الگوریتم رمزنگاری در برابر تغییرات ورودی است. بدین معنا که کوچک‌ترین تغییر در ورودی حتی به‌اندازه یک بیت باید باعث تغییر حداقل ۵۰ درصدی در خروجی شود [۴۱]. این نوع تحلیل دارای دو معیار UACI و NPCR است [۴۲].

NPCR به‌عنوان درصد اختلاف تعداد پیکسل‌های دو تصویر رمز شده است که یکی از تصاویر؛ تصویر اصلی است و تصویر دوم، تصویر اصلی با یک تغییر جزئی خواهد بود. معیار NPCR طبق رابطه (۹) اندازه‌گیری می‌شود.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100$$
$$D(i,j) = \begin{cases} 0 & if\ E(i,j) = \acute{E}(i,j) \\ 1 & if\ E(i,j) \neq \acute{E}(i,j) \end{cases} \qquad (۹)$$

که W و H به ترتیب عرض و طول تصویر، $D(i,j)$ تفاوت بین پیکسل‌های متناظر تصویر رمزگذاری شده تصویر اصلی($E(i,j)$) و تصویر تغییریافته ($\acute{E}(i,j)$) را نشان می دهد.

UACI میانگین اختلاف بین دو تصویر (یک تصویر اصلی و یک تصویر تغییریافته) رمزنگاری شده را اندازه‌گیری می‌کند که طبق رابطه (۱۰) تعریف می‌شود.

$$UACI = \frac{\sum_{i,j} E(i,j) - \acute{E}(i,j)}{255 \times W \times H} \times 100 \qquad (۱۰)$$

در جدول (۱) نتایج آزمایش دو معیار UACI و NPCR برای تصویر رمز شده به ازای هر سه کانال رنگ آورده شده است. مقادیر UACI > ۳۳/۴٪ و NPCR > ۹۹/۶٪ تضمین می‌کند که یک الگوریتم رمزنگاری تصویر در برابر حمله تفاضلی مقاوم است [۴۳].

باتوجه‌به جدول (۱)، الگوریتم رمزنگاری دارای حساسیت مناسبی در برابر تغییرات جزئی است و توانسته است مقادیر بالایی برای دو معیار UACI و NPCR را کسب کند.

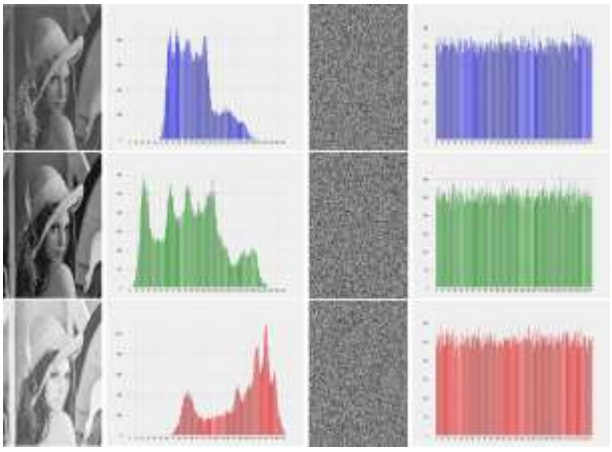
[1] Tournament selection
[2] Boltzmann selection

۴-۲- ۲-۴ تحلیل هیستوگرام

هیستوگرام[3] توزیع مقادیر پیکسل یک تصویر را نشان می‌دهد. هیستوگرام تصویر اصلی باید کاملاً با هیستوگرام تصویر رمزنگاری شده متفاوت باشد.

هیستوگرام تصاویر اصلی ماهیت غیریکنواختی دارند. درحالی‌که هیستوگرام تصاویر رمزنگاری شده باید ماهیت یکنواخت داشته باشند؛ یعنی همه پیکسل‌ها به طور مساوی در فضا توزیع‌شده باشند.

در شکل (۸) هیستوگرام تصویر، قبل و بعد از رمزنگاری ترسیم‌شده است. همان‌طور که گفته شد، هیستوگرام تصویر رمز شده به حالت یکنواخت تبدیل‌شده است.



شکل (۸). نمودار هیستوگرام تصویر نمونه لنا به ازای سه کانال رنگ، قبل و بعد از رمزنگاری

جدول (۱). مقادیر دو معیار NPCR و UACI برای شش تصویر نمونه

تصویر اندازه	معیار	کانال رنگ		
		قرمز	سبز	آبی
Lena 256	NPCR(%)	۹۹/۶۳۱۷	۹۹/۶۵۰۱	۹۹/۶۲۵۹
	UACI(%)	۳۳/۴۱۴۷	۳۳/۴۳۹۸	۳۳/۴۰۳۶
House 256	NPCR(%)	۹۹/۶۰۰۱	۹۹/۶۱۷۲	۹۹/۶۱۶۳
	UACI(%)	۳۳/۴۳۲۵	۳۳/۵۷۰۲	۳۳/۴۱۶۸
Jelly bean 256	NPCR(%)	۹۹/۶۱۶۹	۹۹/۶۲۲۱	۹۹/۶۱۵۶
	UACI(%)	۳۳/۴۱۱۸	۳۳/۴۱۹۸	۳۳/۴۲۶۰
Peppers 512	NPCR(%)	۹۹/۶۰۹۵	۹۹/۶۱۰۳	۹۹/۶۱۱۲
	UACI(%)	۳۳/۴۳۳۵	۳۳/۴۴۷۵	۳۳/۴۴۷۰

[3] Histogram

تصویر اندازه	معیار	کانال رنگ		
		قرمز	سبز	آبی
Mandrill 512	NPCR(%)	۹۹/۶۲۳۵	۹۹/۶۰۸۵	۹۹/۶۰۷۴
	UACI(%)	۳۳/۵۶۳۸	۳۳/۴۶۲۱	۳۳/۴۶۹۲
Aircraft 512	NPCR(%)	۹۹/۶۲۶۷	۹۹/۶۰۵۲	۹۹/۶۱۹۲
	UACI(%)	۳۳/۴۳۴۴	۳۳/۴۳۶۰	۳۳/۴۳۷۳
White 256	NPCR(%)	۹۹/۶۳۵۸	۹۹/۵۹۸۷	۹۹/۶۰۷۳
	UACI(%)	۳۳/۵۳۹۸	۳۳/۴۷۱۶	۳۳/۵۰۱۸
Black 256	NPCR(%)	۹۹/۶۱۵۰	۹۹/۵۸۹۷	۹۹/۶۰۸۱
	UACI(%)	۳۳/۴۲۵۸	۳۳/۳۹۸۳	۳۳/۴۱۹۷

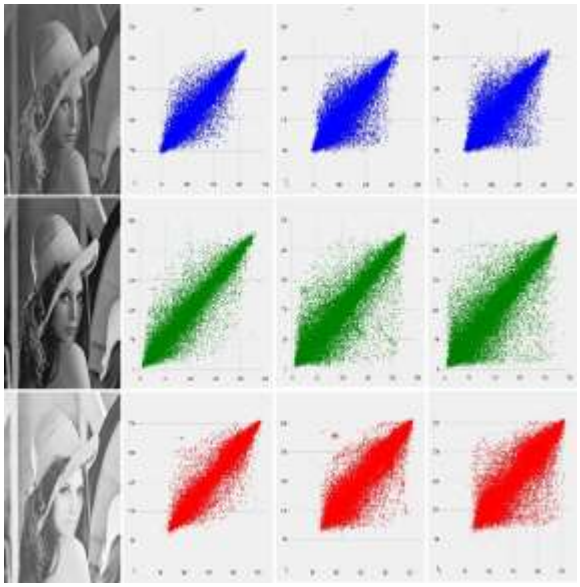
۴-۳- ۳-۴ ضریب همبستگی

ضریب همبستگی برای یافتن شباهت بین پیکسل‌های متناظر یک تصویر اصلی و رمزنگاری شده استفاده می‌شود. مقادیر پیکسل‌های مجاور یک تصویر اصلی در سه جهت افقی، مورب و عمودی دارای ضریب همبستگی بالایی هستند. درحالی‌که یک الگوریتم رمزنگاری مناسب ضریب همبستگی پیکسل‌های تصویر رمز شده را کاهش می‌دهد. ضریب همبستگی طبق رابطه (۱۱) محاسبه می‌شود.

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}}$$
$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K}$$
$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))^2 \qquad (۱۱)$$
$$D(y) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(y))^2$$

که $C(x,y)$ کوواریانس[1]، x و y مختصات تصویر، K تعداد جفت پیکسل‌های (x_i,y_i)، $D(x)$ و $D(y)$ به ترتیب انحراف معیار x و y، و $E(x)$ میانگین پیکسل های x_i است. در جدول (۲)، نتایج میزان همبستگی پیکسل‌های شش تصویر به ازای سه کانال رنگ، و برای هر سه جهت عمودی، افقی و قطری اندازه‌گیری شده است. باتوجه‌به مقادیر جدول (۲)، الگوریتم رمزنگاری به‌خوبی توانسته است همبستگی بین پیکسل‌ها را از بین ببرد.

همچنین برای درک بهتر چگونگی تغییر همبستگی پیکسل‌ها قبل و بعد از رمزنگاری، نمودار نقطه‌ای پیکسل‌ها به‌ازای سه کانال رنگ و سه جهت عمودی، افقی و قطری ترسیم‌شده است که در شکل‌های (۹) و (۱۰) نشان داده‌شده است.باتوجه‌به شکل (۹)، نمودارهای ترسیم‌شده همانند نمودار خطی تابع $f(x) = y$ است. بدین معنا که پیکسل‌ها دارای رابطه‌ای خطی هستند؛ اما در شکل (۱۰)، پس از رمزنگاری تصویر، روابط بین پیکسل‌ها به‌کلی از بین رفته است.



شکل (۹). نمودار نقطه‌ای همبستگی پیکسل‌های سه کانال رنگ برای تصویر لنا

[1] Covariance

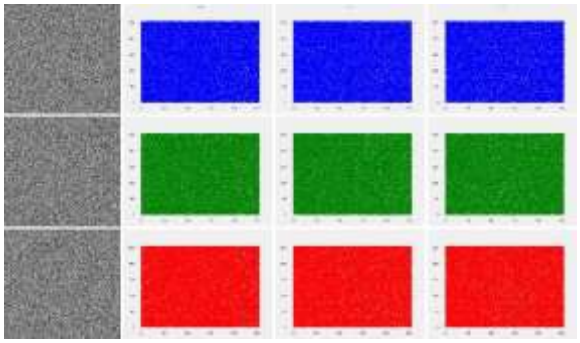
۴-۴- ۴-۴ آنتروپی

آنتروپی میانگین اطلاعات هر بیت در یک تصویر را اندازه‌گیری می‌کند که شامل اطلاعات احتمالی موجود در تصویر است. هر پیکسل مقدار متفاوتی دارد؛ بنابراین، آنتروپی یک تصویر رمزنگاری شده به این معنی است که هر پیکسل احتمال برابری با توزیع یکنواخت دارد. آنتروپی طبق رابطه (۱۲) محاسبه می‌شود.

$$H(S) = -\sum_{s} (P(s_i) \times log_2\ P(s_i)) \qquad (۱۲)$$

که $H(S)$ نشان‌دهنده محاسبه آنتروپی برای داده S، $P(s_i)$ احتمال رخداد s_i است. مقدار آنتروپی برای تصاویر ۸ بیتی بین بازه $[0,8]$ قرار می‌گیرد. برای بررسی میزان آنتروپی تصاویر رمزنگاری شده، آنتروپی شش تصویر نمونه پس از رمزنگاری محاسبه‌شده است و نتایج آن به ازای هر سه کانال رنگ در جدول (۳) آورده شده است.

باتوجه‌به جدول (۳) مقدار آنتروپی تمامی آزمایش‌ها بسیار نزدیک به حد نهایی آنتروپی (عدد ۸) برای یک تصویر ۸ بیتی است.



شکل (۱۰). نمودار نقطه‌ای همبستگی پیکسل‌های سه کانال رنگ برای تصویر رمز شده لنا

جدول (۳). مقدار آنتروپی شش تصویر نمونه پس از رمزنگاری به ازای سه کانال رنگ

تصویر اندازه	آنتروپی		
	قرمز	سبز	آبی
Lena 256	۷/۹۹۶۹	۷/۹۹۷۴	۷/۹۹۷۲
House 256	۷/۹۹۷۳	۷/۹۹۷۱	۷/۹۹۷۴
Jelly bean 256	۷/۹۹۷۲	۷/۹۹۷۱	۷/۹۹۷۰
Peppers 512	۷/۹۹۹۳	۷/۹۹۹۳	۷/۹۹۹۲
Mandrill 512	۷/۹۹۹۴	۷/۹۹۹۱	۷/۹۹۹۲
Aircraft 512	۷/۹۹۹۲	۷/۹۹۹۰	۷/۹۹۹۳
White 256	۷/۹۹۷۴	۷/۹۹۷۲	۷/۹۹۷۰
Black 256	۷/۹۹۷۱	۷/۹۹۷۳	۷/۹۹۶۸

۴-۵- ۴-۵ آزمایش داده‌های ازدست‌رفته

در این آزمایش فرض می‌شود که تصویر رمز شده در زمان انتقال

جدول (۲). مقادیر همبستگی پیکسل‌های کانال‌های رنگ تصاویر

تصویر اندازه	کانال رنگ	جهت همبستگی		
		افقی	عمودی	قطری
Lena 256	قرمز	-۰/۱۸۳۵	-۰/۱۵۴۶	-۰/۰۴۰۳
	سبز	-۰/۰۱۲۴	-۰/۱۸۱۷	-۰/۱۹۰۹
	آبی	-۰/۱۴۹۷	-۰/۰۹۵۹	-۰/۱۵۳۱
House 256	قرمز	-۰/۱۸۸۴	-۰/۱۰۶۰	-۰/۱۱۲۵
	سبز	-۰/۱۵۸۸	-۰/۱۰۰۱	-۰/۱۲۵۳
	آبی	-۰/۱۳۸۲	-۰/۰۹۷۶	-۰/۱۴۶۰
Jelly bean 256	قرمز	-۰/۰۸۲۴	-۰/۲۲۰۸	-۰/۱۹۱۰
	سبز	-۰/۲۶۹۵	-۰/۱۲۷۷	-۰/۰۹۷۳
	آبی	-۰/۰۳۳۴	-۰/۱۴۴۱	-۰/۲۴۴۸
Peppers 512	قرمز	-۰/۱۳۴۲	-۰/۱۹۶۷	-۰/۱۱۹۹
	سبز	-۰/۱۳۴۹	-۰/۱۶۴۷	-۰/۱۲۶۶
	آبی	-۰/۱۰۱۱	-۰/۱۶۷۰	-۰/۱۵۴۸
Mandrill 512	قرمز	-۰/۰۹۹۷	-۰/۱۵۳۲	-۰/۱۲۱۴
	سبز	-۰/۲۰۷۶	-۰/۰۹۸۵	-۰/۱۱۹۲
	آبی	-۰/۱۵۰۷	-۰/۰۸۷۳	-۰/۱۴۶۰
Aircraft 512	قرمز	-۰/۲۰۰۳	-۰/۱۰۳۹	-۰/۱۳۴۶
	سبز	-۰/۱۶۷۴	-۰/۲۵۴۵	-۰/۱۰۴۱
	آبی	-۰/۲۷۱۰	-۰/۱۲۶۹	-۰/۰۷۳۷
White 256	قرمز	-۰/۱۴۹۷	-۰/۱۰۵۸	-۰/۱۷۲۶
	سبز	-۰/۱۸۵۹	-۰/۱۵۳۰	-۰/۱۸۷۱
	آبی	-۰/۱۶۶۲	-۰/۰۹۸۰	-۰/۱۶۶۸
Black 256	قرمز	-۰/۱۵۷۳	-۰/۱۶۹۶	-۰/۱۴۲۰
	سبز	-۰/۱۳۸۹	-۰/۱۸۲۰	-۰/۱۲۳۵
	آبی	-۰/۱۳۶۲	-۰/۱۶۳۰	-۰/۰۹۹۷

به دست فردی مخرب می‌رسد و بخشی از تصویر را تخریب می‌کند که به نام حمله‌برش شناخته می‌شود. در این صورت زمان رمزگشایی تصویر، اطلاعات تصویر از بین رفته است و تصویر رمزگشایی‌شده، متفاوت از تصویر اصلی خواهد بود.

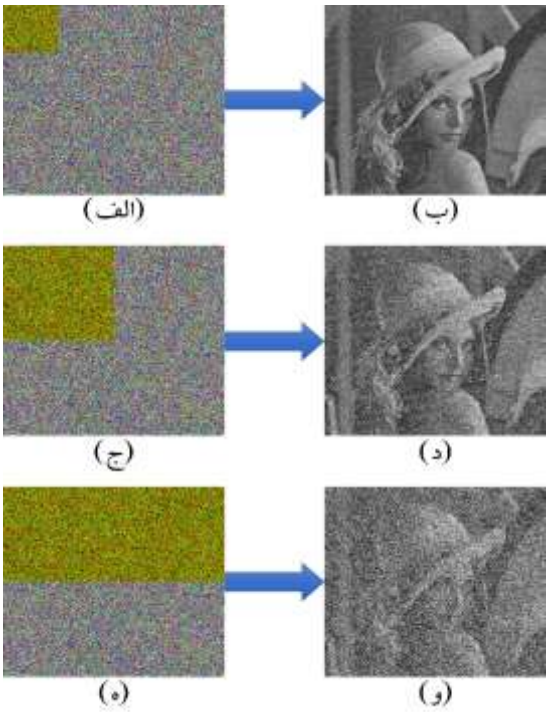
اگر الگوریتم رمزنگاری مناسب باشد (توزیع مناسب پیکسل‌ها، ازبین‌بردن اطلاعات آماری) حتی پس از تخریب بخشی از تصویر، تصویر رمزگشایی‌شده همچنان قابل‌استفاده خواهد بود و تنها بر اساس میزان تخریب، تصویر دچار نویز می‌شود.

به‌منظور سنجش مقاومت الگوریتم رمزنگاری در برابر حمله‌برش، تصویر رمزنگاری شده با درصدهای مختلفی تخریب می‌شود و سپس رمزگشایی می‌شود. نتایج آزمایش با درصد تخریب ۶٪، ۲۵٪ و ۵۰٪ برای کانال آبی تصویر نمونه لنا در تصویر (۱۱) قابل‌مشاهده است.

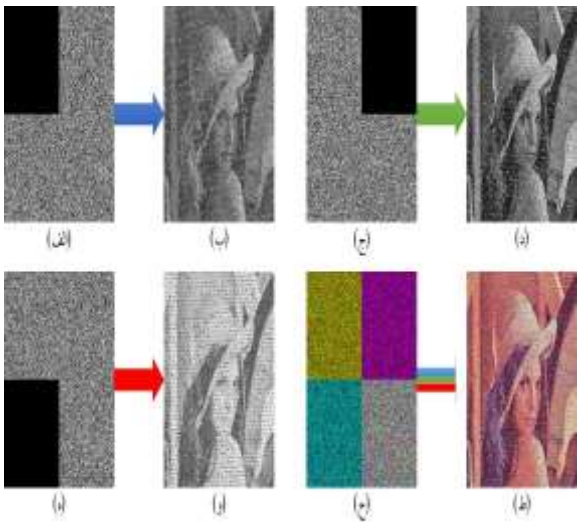
در آزمایش دیگری ۲۵ درصد هر سه کانال رنگ در موقعیت‌های متفاوت تخریب می‌شوند و تصویر رنگی نهایی رمزگشایی می‌شود. نتیجه آزمایش در شکل (۱۲) نشان داده‌شده است.

باتوجه‌به نتایج حاصل‌شده، می‌توان نتیجه گرفت که

الگوریتم رمزنگاری مقاومت مناسبی در برابر حمله‌برش دارد و حتی پس از تخریب بخشی از تصویر، تصویر رمزگشایی‌شده قابل‌استفاده است.



شکل (۱۱). مقاومت الگوریتم رمزنگاری در برابر حمله برش. (الف): تخریب ۶ درصد (ب): رمزگشایی تصویر «الف» (ج): تخریب ۲۵ درصد (د): رمزگشایی تصویر «ج» (ه): تخریب ۵۰ درصد (و): رمزگشایی تصویر «ه»



شکل (۱۲). مقاومت الگوریتم رمزنگاری در برابر حمله برش. (الف): تخریب ۲۵ درصد کانال آبی (ب): رمزگشایی تصویر «الف» (ج): تخریب ۲۵ درصد کانال سبز (د): رمزگشایی تصویر «ج» (ه): تخریب ۲۵ درصد کانال قرمز (و): رمزگشایی تصویر «ه» (ح): ترکیب کانال‌های رنگ رمز شده (ط): رمزگشایی تصویر «ح»

جدول (۴). کلیدهای رمز تغییریافته

کلید رمز	پارامترهای کلید
Key 1	$\{main\ \acute{v}ector,\ \sigma, \rho, \beta, a_b, b_b, a_g, b_g, a_r, b_r\}$
Key 2	$\{main\ vector,\ \acute{\sigma}, \rho, \beta, a_b, b_b, a_g, b_g, a_r, b_r\}$
Key 3	$\{main\ vector,\ \sigma, \acute{\rho}, \beta, a_b, b_b, a_g, b_g, a_r, b_r\}$
Key 4	$\{main\ vector,\ \sigma, \rho, \acute{\beta}, a_b, b_b, a_g, b_g, a_r, b_r\}$
Key 5	$\{main\ vector,\ \sigma, \rho, \beta, \acute{a_b}, b_b, a_g, b_g, a_r, b_r\}$
Key 6	$\{main\ vector,\ \sigma, \rho, \beta, a_b, \acute{b_b}, a_g, b_g, a_r, b_r\}$
Key 7	$\{main\ vector,\ \sigma, \rho, \beta, a_b, b_b, \acute{a_g}, b_g, a_r, b_r\}$
Key 8	$\{main\ vector,\ \sigma, \rho, \beta, a_b, b_b, a_g, \acute{b_g}, a_r, b_r\}$
Key 9	$\{main\ vector,\ \sigma, \rho, \beta, a_b, b_b, a_g, b_g, \acute{a_r}, b_r\}$
Key 10	$\{main\ vector,\ \sigma, \rho, \beta, a_b, b_b, a_g, b_g, a_r, \acute{b_r}\}$

جدول (۵). مقادیر NPCR برای تصویر رمز شده با کلید اصلی و تغییریافته.

کلید رمز	NPCR		
	قرمز	سبز	آبی
Key 1	۹۹/۶۰۴۶	۹۹/۵۸۷۰	۹۹/۵۹۳۰
Key 2	۹۹/۵۸۸۰	۹۹/۶۰۰۲	۹۹/۶۰۴۸
Key 3	۹۹/۶۰۴۲	۹۹/۶۱۶۴	۹۹/۵۸۵۱
Key 4	۹۹/۶۱۱۲	۹۹/۶۲۰۳	۹۹/۵۸۷۲
Key 5	۹۹/۶۰۴۰	۹۹/۵۸۶۷	۹۹/۵۸۱۶
Key 6	۹۹/۵۹۵۲	۹۹/۵۹۸۴	۹۹/۶۱۹۲
Key 7	۹۹/۵۸۵۵	۹۹/۵۸۲۸	۹۹/۶۲۹۱
Key 8	۹۹/۵۹۹۸	۹۹/۶۰۵۰	۹۹/۶۱۰۸
Key 9	۹۹/۶۰۸۵	۹۹/۶۲۶۲	۹۹/۶۱۴۸
Key 10	۹۹/۶۱۹۹	۹۹/۶۱۰۳	۹۹/۶۰۹۸

۴-۶- ۶-۴ تحلیل کلید رمز

همان‌طور که در بخش ۳-۷ اشاره شد، کلید رمزنگاری برای تصاویر رنگی و خاکستری، به ترتیب دارای ۸۰۰ و ۷۳۶ بیت است؛ بنابراین باتوجه‌به طول مناسب کلید، الگوریتم رمزنگاری در برابر حمله Brute Force مقاوم خواهد بود. از طرفی بخش ابتدایی کلید (۵۱۲ بیت ابتدا) چکیده سه داده کلید عمومی، بردار ویژگی‌های چهره و تصویر اصلی است؛ بنابراین تغییر یک بیت در داده‌های ذکرشده منجر به تغییر کل کلید رمز می‌شود، زیرا مقادیر اولیه نگاشت لورنز، از چکیده داده‌ها حاصل می‌شود. برای بررسی حساسیت الگوریتم رمزنگاری نسبت به کلید رمز، ابتدا تصویر نمونه را با کلید اصلی

$$Key = \{main\ vector, \sigma, \rho, \beta, a_b, b_b, a_g, b_g, a_r, b_r\}$$

رمزنگاری می‌شود. سپس هر بخش از کلید به طور مستقل دچار تغییری جزئی می‌شود و مابقی بخش‌های کلید ثابت می‌مانند. کلیدهای حاصل در جدول (۴) نشان داده‌شده‌اند.

تصویر لنا با هرکدام از کلیدها جداگانه رمزنگاری می‌شود. میزان NPCR هرکدام از تصاویر رمزنگاری شده با کلیدهای تغییریافته، با تصویر رمز شده توسط کلید اصلی محاسبه می‌شود. نتایج آزمایش در جدول (۵) نشان داده‌شده است.

باتوجه‌به مقادیر جدول (۵)، الگوریتم رمزنگاری حساسیت بالایی نسبت به تغییرات جزئی کلید دارد و با تغییر هر بخش از کلید رمز، تصویر رمز شده حاصل متفاوت خواهد بود.

۴-۷- ۴-۷ مقایسه نتایج الگوریتم پیشنهادی با سایر روش‌ها

در این بخش نتایج به‌دست‌آمده از روش پیشنهادی با سایر روش‌های ارائه‌شده درزمینهٔ رمزنگاری تصویر مقایسه می‌شود. نتایج مقایسه میزان همبستگی پیکسل‌های تصویر رمز شده، حملات تفاضلی و آنتروپی در جدول (۶) آورده شده است.

روش‌هایی که در جدول (۶) برای ارزیابی با روش پیشنهادی معرفی شده‌اند، در فاز جای‌گشت از روش‌هایی مانند مرتب سازی دنباله آشوب، عملگرهای همبری و جهش الگوریتم ژنتیک و مربع لاتین استفاده کرده‌اند. اما در روش پیشنهادی از الگوریتم فراابتکاری ژنتیک و نگاشت آشوب آرنولد جهت بهینه‌سازی همبستگی پیکسل‌ها استفاده شده است. باتوجه‌به جدول (۶)، روش پیشنهادی در مقایسه با سایر روش‌ها، بسیار موفق عمل کرده است و توانسته است همبستگی پیکسل‌ها را به‌صورت چشمگیری کاهش دهد؛ بنابراین روش پیشنهادی در مقابل حملات آماری مقاومت بالایی خواهد داشت. باتوجه‌به جدول (۶)، روش پیشنهادی در معیار همبستگی پیکسل‌ها در مقایسه با سایر روش‌ها، بسیار موفق عمل کرده است و توانسته است همبستگی پیکسل‌ها را در هر سه جهت افقی، عمودی و قطری به‌صورت چشمگیری کاهش دهد؛ بنابراین روش پیشنهادی در مقابل حملات آماری مقاومت بالایی خواهد داشت. همچنین روش‌هایی که برای ارزیابی با روش پیشنهادی انتخاب شده‌اند در فرآیند رمزنگاری از روش‌هایی مانند عملیات حسابی تنسورها، کدگذاری DNA، چکیده تصویر، دنباله‌های آشوب و عملگرهای الگوریتم ژنتیک استفاده کرده‌اند. باتوجه‌به اینکه در روش پیشنهادی از روش‌های چکیده تصویر، نگاشت‌های آشوب و الگوریتم فراابتکاری ژنتیک استفاده شده است، روش پیشنهادی توانسته است در آزمایش‌هایی موفق‌تر عمل کند و قابلیت رقابت با روش‌های مشابه را داشته باشد؛ بنابراین روش پیشنهادی در مقایسه با سایر روش‌های مشابه توانسته است نتایج مناسبی در آزمایش آنتروپی و تحلیل تفاضلی کسب کند.

۵- نتیجه‌گیری

در این مقاله یک روش جدید رمزنگاری تصویر مبتنی بر ویژگی‌های بیومتریک چهره و زنجیره‌بلوکی ارائه شده است که در فاز جانشینی از سه داده چکیده تصویر اصلی، بردار ویژگی‌های چهره و کلید عمومی برای تولید دنباله‌های شبه‌تصادفی استفاده شده است؛ بنابراین مقادیر دنباله‌ها بسیار وابسته به سه داده ذکرشده هستند و با تغییر یک بیت در هرکدام از داده‌ها، مقادیر دنباله‌های شبه‌تصادفی به‌کلی تغییر می‌کند. فاز جای‌گشت با استفاده از الگوریتم فراابتکاری ژنتیک کاراتر و بهینه‌تر انجام شد. در این فاز ابتدا یک جمعیت اولیه ساخته می‌شود که هرکدام از اعضای جمعیت دارای دو متغیر (دو متغیر نگاشت آرنولد) است.

تصویر توسط نگاشت آرنولد به‌ازای هرکدام از اعضای جمعیت جای‌گشت داده می‌شود و در هر مرحله جمعیت جدید بر اساس شایستگی ساخته می‌شود. پس از رسیدن به‌شرط توقف الگوریتم ژنتیک، بهترین عضو انتخاب، و تصویر جای‌گشت داده می‌شود. تابع شایستگی، مجموع وزن‌دار سه مقدار همبستگی پیکسل‌ها (افقی، عمودی و قطری) است. باتوجه‌به نتایج حاصل که در بخش ۴ بررسی شدند، الگوریتم رمزنگاری تأثیر چشمگیری در کاهش میزان همبستگی پیکسل‌ها و ازبین‌بردن اطلاعات آماری تصویر داشته است. همچنین نتایج آزمایش‌های مختلف انجام‌شده در بخش ۴، نشان می‌دهد که روش پیشنهادی در مقابل حملات آماری، حملات تفاضلی، حمله‌برش و حمله Brute Force مقاوم است.

پس از رمزنگاری تصویر، کلید رمزنگاری و بردار ویژگی‌های چهره توسط کلید عمومی رمزنگاری می‌شوند و به‌عنوان یک تراکنش در شبکه زنجیره‌بلوکی ذخیره می‌شوند. به‌منظور رمزگشایی تصویر یک فرآیند احراز هویت دومرحله‌ای انجام می‌پذیرد. در اولین مرحله با استفاده از کلید عمومی و خصوصی و در دومین مرحله به‌وسیلهٔ انطباق چهره کاربر، هویت فرد رمزنگار مشخص می‌شود که در صورت صحت هویت کاربر، کلید رمزنگاری در اختیارش قرار می‌گیرد.

در انتها باتوجه‌به ارزیابی‌ها و مقایسه‌هایی که برای روش پیشنهادی و سایر روش‌های مشابه که در بخش ۴-۷ انجام شد، می‌توان نتیجه گرفت که بخش‌های مختلف روش پیشنهادی مانند نگاشت‌های آشوب، الگوریتم ژنتیک، چکیده اطلاعات تصویر و چهره، کلید رمز، استراتژی رمزنگاری و احرازهویت به خوبی درکنار یکدیگر قرار گرفته‌اند و یک سیستم با عملکرد مناسب را شکل داده‌اند. باتوجه‌به جدول (۶)، روش پیشنهادی توانسته است یکی از اهداف اصلی الگوریتم رمزنگاری یعنی همبستگی پیکسل‌ها را به طور چشمگیری، نسبت به سایر روش‌های مقایسه شده کاهش دهد. همچنین الگوریتم پیشنهادی در معیارهای تفاضلی و آماری نیز توانسته است نتایج مناسبی را به دست آورد و در بسیاری از نتایج از روش‌های مشابه عملکرد بهتری داشته باشد.

جدول (۶). مقایسه نتایج روش پیشنهادی با سایر روش‌ها

تصویر کانال رنگ	معیار ارزیابی		الگوریتم					
			[۱۳]	[۱۴]	[۱۸]	[۲۴]	[۲۵]	روش پیشنهادی
لنا کانال قرمز	آنتروپی		۷/۹۹۷۲	۷/۹۹۱۷	۷/۹۹۹۴	۷/۹۹۷۳	۷/۹۹۷۲	۷/۹۹۶۹
	ضریب همبستگی	افقی	۰/۰۰۹۴	۰/۰۰۱۳	-۰/۰۰۰۲	۰/۰۰۴۶	۰/۰۰۸۳	-۰/۱۸۳۵
		عمودی	-/۰۰۱۱	۰/۰۰۴۷	-۰/۰۰۲۳	۰/۰۰۲۴	-۰/۰۰۵۴	-۰/۱۵۴۶
		قطری	۰/۰۰۰۹	۰/۰۰۰۲	-۰/۰۰۲۱	۰/۰۰۵۱	-۰/۰۰۱۰	-۰/۰۴۰۳
	تحلیل تفاضلی	NPCR	۹۹/۶۴۹۱	۹۹/۶۲۴۳	۹۹/۶۰۹۶	۹۹/۶۶۱۹	۹۹/۶۰۷۸	۹۹/۶۳۱۷
		UACI	۳۳/۳۸۲۷	۳۳/۴۲۲۴	۳۳/۴۵۹۹	۳۳/۶۱۷۷	۳۳/۵۶۴۴	۳۳/۴۱۴۷
لنا کانال سبز	آنتروپی		۷/۹۹۶۸	۷/۹۹۱۲	۷/۹۹۹۴	۷/۹۹۷۰	۷/۹۹۷۲	۷/۹۹۷۴
	ضریب همبستگی	افقی	-۰/۰۰۱۸	۰/۰۰۳۲	-۰/۰۰۰۲	-۰/۰۰۲۷	۰/۰۰۴۹	-۰/۰۱۲۴
		عمودی	-۰/۰۰۷۶	-۰/۰۰۰۵	-۰/۰۰۴۳	-۰/۰۰۰۷	۰/۰۱۰۰	-۰/۱۸۱۷
		قطری	۰/۰۰۰۶	۰/۰۰۴۸	۰/۰۰۰۷	-۰/۰۰۰۲	۰/۰۱۲۴	-۰/۱۹۰۹
	تحلیل تفاضلی	NPCR	۹۹/۶۱۶۳	۹۹/۶۱۸۵	۹۹/۶۱۰۷	۹۹/۶۲۷۲	۹۹/۶۶۷۸	۹۹/۶۵۰۱
		UACI	۳۳/۳۶۶۱	۳۳/۴۳۶۱	۳۳/۴۷۶۷	۳۳/۶۰۴۸	۳۳/۴۴۵۸	۳۳/۴۳۹۸
لنا کانال آبی	آنتروپی		۷/۹۹۷۶	۷/۹۹۱۷	۷/۹۹۹۴	۷/۹۹۷۲	۷/۹۹۷۵	۷/۹۹۷۲
	ضریب همبستگی	افقی	۰/۰۰۱۹	۰/۰۰۲۰	-۰/۰۰۷۴	-۰/۰۰۲۳	-۰/۰۰۱۷	-۰/۱۴۹۷
		عمودی	-۰/۰۰۴۲	۰/۰۰۰۱	-۰/۰۰۱۰	۰/۰۰۱۴	۰/۰۰۹۵	-۰/۰۹۵۹
		قطری	۰/۰۰۲۲	-۰/۰۰۴۰	-۰/۰۰۰۷	۰/۰۰۰۴	-۰/۰۰۴۲	-۰/۱۵۳۱
	تحلیل تفاضلی	NPCR	۹۹/۶۳۲۴	۹۹/۶۲۸۰	۹۹/۶۰۹۰	۹۹/۶۴۶۰	۹۹/۶۰۷۸	۹۹/۶۲۵۹
		UACI	۳۳/۴۵۷۷	۳۳/۴۶۰۳	۳۳/۴۳۳۳	۳۳/۶۴۲۲	۳۳/۵۰۵۵	۳۳/۴۰۳۶

۶- مراجع

[1]. M. Turculeț, "Ethical Issues Concerning Online Social Networks," *Procedia Soc Behav Sci*, vol. 149, pp. 967–972, 2014, doi: https://doi.org/10.1016/j.sbspro.2014.08.317.

[2]. S. Lian, *Multimedia content encryption: techniques and applications*. Auerbach Publications, 2008.

[3]. X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf Sci (N Y)*, vol. 486, pp. 340–358, Jun. 2019, doi: 10.1016/J.INS.2019.02.049.

[4]. H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 144, pp. 444–452, Mar. 2018, doi: 10.1016/J.SIGPRO.2017.11.005.

[5]. D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," *Signal Processing*, vol. 206, p. 108908, May 2023, doi: 10.1016/J.SIGPRO.2022.108908.

[6]. H. Ghadirli, A. Nodehi, R. E.-S. Processing, and undefined 2019, "An overview of encryption algorithms in color images," *Elsevier*, vol. 164, pp. 163–185, 2019, doi: 10.1016/j.sigpro.2019.06.010.

[7]. X. Wang and M. Zhao, "An image encryption algorithm based on hyperchaotic system and DNA coding," *Opt Laser Technol*, vol. 143, p. 107316, Nov. 2021, doi: 10.1016/J.OPTLASTEC.2021.107316.

[8]. S. Ma, Y. Zhang, Z. Yang, J. Hu, and X. Lei, "A New Plaintext-Related Image Encryption Scheme Based on Chaotic Sequence," *IEEE Access*, vol. 7, pp. 30344–30360, 2019, doi: 10.1109/ACCESS.2019.2901302.

[9]. X. J. Tong, M. Zhang, Z. Wang, Y. Liu, H. Xu, and J. Ma, "A fast encryption algorithm of color image based on four-dimensional chaotic system," *J Vis Commun Image Represent*, vol. 33, pp. 219–234, Nov. 2015, doi: 10.1016/J.JVCIR.2015.09.014.

[10]. N. Khalil, A. Sarhan, and M. A. M. Alshewimy, "An

color image encryption scheme based on 2DNLCML system and genetic operations," *Opt Lasers Eng*, vol. 128, p. 106040, May 2020, doi: 10.1016/J.OPTLASENG.2020.106040.

[25]. X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, "Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption," *Signal Processing*, vol. 183, p. 108041, Jun. 2021, doi: 10.1016/J.SIGPRO.2021.108041.

[26]. L. S. Khan, M. M. Hazzazi, M. Khan, and S. S. Jamal, "A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes," *Chinese Journal of Physics*, vol. 72, pp. 558–574, Aug. 2021, doi: 10.1016/J.CJPH.2021.03.029.

[27]. Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain," *Opt Laser Technol*, vol. 135, p. 106610, Mar. 2021, doi: 10.1016/J.OPTLASTEC.2020.106610.

[28]. R. Li, "Fingerprint-related chaotic image encryption scheme based on blockchain framework," *Multimed Tools Appl*, vol. 80, no. 20, pp. 30583–30603, Aug. 2021, doi: 10.1007/S11042-020-08802-Z/METRICS.

[29]. G. Boeing, "Visual Analysis of Nonlinear Dynamical Systems: Chaos, Fractals, Self-Similarity and the Limits of Prediction," *Systems 2016, Vol. 4, Page 37*, vol. 4, no. 4, p. 37, Nov. 2016, doi: 10.3390/SYSTEMS4040037.

[30]. N. A. Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map," *Egyptian Informatics Journal*, vol. 17, no. 1, pp. 139–146, Mar. 2016, doi: 10.1016/J.EIJ.2015.10.001.

[31]. G. Qu *et al.*, "Optical color image encryption based on Hadamard single-pixel imaging and Arnold transformation," *Opt Lasers Eng*, vol. 137, p. 106392, Feb. 2021, doi: 10.1016/J.OPTLASENG.2020.106392.

[32]. E. N. Lorenz, "Deterministic Nonperiodic Flow," *J Atmos Sci*, vol. 20, no. 2, pp. 130–141, Mar. 1963, doi: 10.1175/1520-0469(1963)020.

[33]. S. Katoch, S. S. Chauhan, and V. Kumar, "A review on genetic algorithm: past, present, and future," *Multimed Tools Appl*, vol. 80, no. 5, pp. 8091–8126, Feb. 2021, doi: 10.1007/S11042-020-10139-6/FIGURES/8.

[34]. A. Bodo, "Method for producing a digital signature with aid of a biometric feature," *German patent DE*, vol. 42, no. 43, p. 908, 1994.

[35]. V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, Dec. 2019, doi: 10.1007/S41939-019-00049-Y/METRICS.

[36]. C. Bisogni, G. Iovane, R. E. Landi, and M. Nappi, "ECB2: A novel encryption scheme using face biometrics for signing blockchain transactions," *Journal of Information Security and Applications*, vol. 59, p. 102814, Jun. 2021, doi: 10.1016/J.JISA.2021.102814.

[37]. N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," *Proceedings - 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR 2005*, vol. I, pp. 886–893, 2005, doi: 10.1109/CVPR.2005.177.

[38]. O. Déniz, G. Bueno, J. Salido, and F. De La Torre, "Face recognition using Histograms of Oriented Gradients," *Pattern Recognit Lett*, vol. 32, no. 12, pp. 1598–1603, Sep. 2011, doi: 10.1016/J.PATREC.2011.01.004.

[39]. K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint Face efficient color/grayscale image encryption scheme based on hybrid chaotic maps," *Opt Laser Technol*, vol. 143, p. 107326, Nov. 2021, doi: 10.1016/J.OPTLASTEC.2021.107326.

[11]. T. Wang and M. hui Wang, "Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding," *Opt Laser Technol*, vol. 132, p. 106355, Dec. 2020, doi: 10.1016/J.OPTLASTEC.2020.106355.

[12]. S. Zhou, "A real-time one-time pad DNA-chaos image encryption algorithm based on multiple keys," *Opt Laser Technol*, vol. 143, p. 107359, Nov. 2021, doi: 10.1016/J.OPTLASTEC.2021.107359.

[13]. J. Zhou, N.-R. Zhou, and L.-H. Gong, "Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix," *Opt Laser Technol*, vol. 131, p. 106437, Nov. 2020, doi: 10.1016/J.OPTLASTEC.2020.106437.

[14]. D. Zhang, L. Chen, and T. Li, "Hyper-Chaotic Color Image Encryption Based on Transformed Zigzag Diffusion and RNA Operation," *Entropy 2021, Vol. 23, Page 361*, vol. 23, no. 3, p. 361, Mar. 2021, doi: 10.3390/E23030361.

[15]. H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Processing*, vol. 113, pp. 104–112, Aug. 2015, doi: 10.1016/J.SIGPRO.2015.01.016.

[16]. X. Chai, X.-L. Chai, Z.-H. Gan, Y. Lu, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *iopscience.iop.org*, vol. 25, no. 10, p. 100503, 2016, doi: 10.1088/1674-1056/25/10/100503.

[17]. E. Zarei Zefreh, "An Image Encryption Algorithm Based on the Sn Permutation Group and Chaotic Functions" *Journal of Electronical & Cyber Defence*, vol. 8, no. 3, pp.139–150,2020,dor: 20.1001.1.23224347.1399.8.3.11.5 (In Persian)

[18]. Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimed Tools Appl*, vol. 80, no. 9, pp. 13841–13864, Apr. 2021, doi: 10.1007/S11042-020-10437-Z/METRICS.

[19]. S. Zhou, X. Wang, Y. Zhang, B. Ge, M. Wang, and S. Gao, "A novel image encryption cryptosystem based on true random numbers and chaotic systems," *Multimed Syst*, vol. 28, no. 1, pp. 95–112, Feb. 2022, doi: 10.1007/S00530-021-00803-8.

[20]. R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata," *Opt Lasers Eng*, vol. 71, pp. 33–41, Aug. 2015, doi: 10.1016/J.OPTLASENG.2015.03.007.

[21]. R. Enayatifar, A. H. Abdullah, and M. Lee, "A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption," *Opt Lasers Eng*, vol. 51, no. 9, pp. 1066–1077, Sep. 2013, doi: 10.1016/J.OPTLASENG.2013.03.010.

[22]. S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, "Optimizing chaos based image encryption," *Multimed Tools Appl*, vol. 77, no. 19, pp. 25569–25590, Oct. 2018, doi: 10.1007/S11042-018-5807-X.

[23]. A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *AEU - International Journal of Electronics and Communications*, vol. 66, no. 10, pp. 806–816, Oct. 2012, doi: 10.1016/J.AEUE.2012.01.015.

[24]. Y. Q. Zhang, Y. He, P. Li, and X. Y. Wang, "A new

Detection and Alignment Using Multitask Cascaded Convolutional Networks," *IEEE Signal Process Lett*, vol. 23, no. 10, pp. 1499–1503, Oct. 2016, doi: 10.1109/LSP.2016.2603342.

[40]. F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 07-12-June-2015, pp. 815–823, Oct. 2015, doi: 10.1109/CVPR.2015.7298682.

[41]. H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Processing*, vol. 164, pp. 163–185, Nov. 2019, doi: 10.1016/J.SIGPRO.2019.06.010.

[42]. M. Kaur and V. Kumar, "A Comprehensive Review on Image Encryption Techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, Jan. 2020, doi: 10.1007/S11831-018-9298-8/METRICS.

[43]. M. Essaid, I. Akharraz, A. Saaidi, and A. Mouhib, "A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map," *Procedia Comput Sci*, vol. 127, pp. 539–548, Jan. 2018, doi: 10.1016/J.PROCS.2018.01.153.

"پدافند الکترونیکی و سایبری"
سال دوازدهم، شماره ۲، تابستان ۱۴۰۳، ص ۸۳-۶۷

علمی – پژوهشی

رمزنگاری تصویر با استفاده از بیومتریک چهره و الگوریتم فراابتکاری بر روی سیستم زنجیره‌بلوکی

محمد گنجعلیخان حاکمی [۱]، محمدجواد رستمی [۲*]

۱- کارشناسی ارشد، ۲- استادیار، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه شهید باهنر کرمان، کرمان، ایران.

(دریافت: ۱۴۰۳/۰۲/۰۸، بازنگری: ۱۴۰۳/۰۳/۲۹، پذیرش: ۱۴۰۳/۰۵/۱۲، انتشار: ۱۴۰۳/۰۶/۱۳)

DOR:

ناشر: دانشگاه جامع امام حسین (ع) نویسندگان

چکیده

با گسترش شبکه اینترنت و دسترسی همگانی به این شبکه، میزان تبادل اطلاعات و داده‌ها روزبه‌روز افزایش می‌یابد؛ بنابراین، امکان دسترسی غیرمجاز به اطلاعاتی که مبادله می‌شوند وجود خواهد داشت. از طرفی تقریباً تمام برنامه‌هایی که بر بستر اینترنت اجرا می‌شوند، مانند شبکه-های اجتماعی، دسترسی کامل به تصاویر و محتوای ذخیره‌شده در دستگاه میزبان را دارا هستند؛ بنابراین امکان دسترسی غیرمجاز و سرقت اطلاعات شخصی وجود دارد. ازاین‌رو باید امنیت و صحت اطلاعات تضمین شود. به‌منظور حفظ محرمانگی داده‌ها می‌توان از روش‌های رمزنگاری اطلاعات، مانند الگوریتم‌های رمزنگاری تصویر استفاده کرد. در روش پیشنهادی این مقاله کلید الگوریتم رمزنگاری به کمک اطلاعات استخراج‌شده از چهره فرد، چکیده تصویر و کلید عمومی ایجاد می‌شود، بنابراین الگوریتم رمزنگاری نسبت به تغییر هر کدام از اطلاعات استفاده شده در تولید کلید حساسیت بالایی خواهد داشت. برای رمزنگاری تصویر در فاز جانشینی از نگاشت آشوب لورنز استفاده می‌شود. هر کانال رنگ تصویر به چهار قسمت تقسیم می‌شود و هر قسمت با استفاده از یک دنباله شبه‌تصادفی مجزا رمزنگاری می‌شود و تصویر رمز شده تولید می‌شود. در فاز جای‌گشت به‌منظور دست‌یافتن به بهترین تصویر رمز شده، از الگوریتم فراابتکاری ژنتیک (GA) استفاده می‌شود تا با انتخاب پارامترهای بهینه برای نگاشت آشوب آرنولد، مقدار همبستگی پیکسل‌های تصویر رمزنگاری شده به حداقل مقدار ممکن نزدیک شود. باتوجه‌به نتایج به‌دست‌آمده، مقادیر همبستگی پیکسل‌ها در هر سه جهت افقی، عمودی و قطری نسبت به سایر روش‌های ارائه شده مشابه بسیار کوچک‌تر است و الگوریتم رمزنگاری توانسته است به طور چشمگیری همبستگی و ارتباط بین پیکسل‌ها را کاهش دهد. همچنین باتوجه‌به نتایج تحلیل تفاضلی NPCR و UACI، برای تمام تصاویر آزمایش شده به ترتیب بالاتر از ۹۹/۶ درصد و ۳۳/۴ درصد است؛ بنابراین روش پیشنهادی دارای مقاومت بالایی نسبت به حملات آماری و تفاضلی خواهد داشت. همچنین برای فرآیند رمزگشایی تصویر، از احراز هویت دومرحله‌ای و نگهداری ایمن کلید رمزنگاری در شبکه زنجیره‌بلوکی استفاده می‌شود.

کلیدواژه‌ها: رمزنگاری تصویر، نگاشت آشوب، الگوریتم ژنتیک، احراز هویت، زنجیره‌بلوکی

۱- مقدمه

امروزه با گسترش شبکه‌های ارتباطی و اینترنت، حجم بسیار زیادی از اطلاعات در حال تولید و انتقال است که این امر منجر به اهمیت یافتن مسئلهٔ امنیت و صحت اطلاعات شده است. امنیت اطلاعات به معنی حفاظت اطلاعات، از فعالیت‌های غیرمجازی مانند دسترسی، استفاده، خواندن و یا تغییر اطلاعات است. برای حراست از اطلاعات، باید دسترسی به اطلاعات کنترل شود و فقط افراد مجاز باید توانایی دسترسی به اطلاعات را داشته باشند. به‌عنوان‌مثال از زمان ظهور شبکه‌های اجتماعی اولیه در اوایل سال ۲۰۰۰، شبکه‌های اجتماعی آنلاین به طور گسترده‌ای گسترش‌یافته‌اند که از معروف‌ترین این رسانه‌های اجتماعی در اواسط دهه ۲۰۱۰ فیس‌بوک[۲]، اینستاگرام[۳]، توییتر[۴] و اسنپ چت[۵] را می‌توان نام برد.

حجم عظیم اطلاعات شخصی که به‌صورت آنلاین در دسترس است و در فضای ابری ذخیره‌شده است، باعث شده که توانایی پایگاه‌داده‌ها در ذخیره‌سازی ایمن چنین اطلاعات شخصی کاهش

* رایانامه نویسنده مسئول: rostami@uk.ac.ir

[2] Facebook
[3] Instagram
[4] Twitter
[5] Snapchat

یابد و حفظ حریم خصوصی کاربران در اولویت قرار گیرد. آگاهی و مرزهای نقض حریم خصوصی، می‌تواند جز نگرانی‌های اساسی در عصر فنّاوری باشد [۱]. بخش بزرگی از داده‌های کاربران شامل تصاویر شخصی، مدارک مهم که به‌صورت فایل تصویری و یا متنی و... هستند که معمولاً در تلفن‌های همراه، رایانه‌های شخصی و دیسک‌های ذخیره‌سازی اطلاعات نگهداری می‌شوند. این نوع نگهداری از داده‌ها به دلایل زیادی می‌تواند خطرناک باشند ازجمله‌ی این دلایل می‌توان به هک شدن و یا ویروسی شدن دستگاه‌های نگهداری اطلاعات اشاره کرد؛ بنابراین استفاده از روش‌هایی که امنیت داده‌ها را نتیجه می‌دهند امری ضروری است.

یک از این روش‌ها رمزنگاری اطلاعات است [۲]. از مشهورترین و پرکاربردترین الگوریتم‌های رمزنگاری متقارن می‌توان به AES، DES، IDEA اشاره کرد. از مهم‌ترین الگوریتم‌های رمزنگاری کلید عمومی نیز می‌توان به RSA، ElGamal اشاره کرد که معمولاً برای داده‌هایی با ساختار متنی مورداستفاده قرار می‌گیرند؛ اما در رمزنگاری تصویر، به علت ساختار متفاوت تصاویر، که شامل وابستگی بالای اطلاعات پیکسل‌ها و اطلاعات آماری است، استفاده از روش‌های رمزنگاری متداول مناسب نخواهد بود [۳, ۴]. روش‌های مناسب برای تأمین امنیت تصاویر معمولاً در دودسته کلی قرار می‌گیرند: الف) پنهان کردن اطلاعات، که شامل پنهان نگاری[1] است، که در آن داده‌های مهم، درون داده‌های یک رسانه دیگر مثل تصویر یا ویدئو که رسانه پوششی[2] نام دارد پنهان می‌شود. بنابراین در ظاهر فقط یک تصویر یا ویدئو معمولی دیده می‌شود ولی در واقعیت اطلاعات مهمی در رسانه پوششی قرارگرفته شده است [۵]. ب) رمزنگاری[3]، که شامل تکنیک‌های آشوب، دنباله‌های DNA و... است [۶]. اغلب الگوریتم‌های رمزنگاری تصویر شامل دو مرحله اصلی هستند: مرحله جای‌گشت[4] و مرحله جانشینی[5]. در مرحله جای‌گشت فقط موقعیت پیکسل‌ها با یکدیگر جابجا می‌شوند و در مرحله جانشینی مقادیر پیکسل‌ها تغییر می‌کنند [۷]. پرکاربردترین تکنیک‌های استفاده‌شده در رمزنگاری تصویر شامل نگاشت‌های آشوب[6]، دنباله‌های DNA، چکیده تصویر و الگوریتم های فراابتکاری[7] است [۶]. نگاشت‌های آشوب جزء پرکاربردترین تکنیک‌ها در رمزنگاری تصویر هستند، که می‌توان در هر دو مرحله جانشینی و جای‌گشت از آن‌ها بهره برد [۸].

تانگ و همکارانش [۹] روشی به‌منظور افزایش سرعت و امنیت، رمزنگاری تصویر مبتنی بر سیستم آشوب ۴ بعدی ارائه دادند. در این روش نگاشت ۴ بعدی پیشنهادی، از ترکیب معادلات دو نگاشت سه‌بعدی لورنز[8] و چن[9] به دست می‌آید. به‌منظور رمزنگاری پیکسل‌های تصویر، ابتدا توسط نگاشت آشوب پیشنهادی، چهار دنباله آشوب تولید می‌شود. در این الگوریتم سعی می‌شود از دنباله‌های تولیدشده مجدد استفاده شود و به تعداد پیکسل‌های تصویر اعداد تصادفی دنباله تولید نشود؛ بنابراین تعدادی معین از اعداد دنباله‌ها انتخاب می‌شود و با قسمت ده‌دهی این اعداد سه کلید متفاوت ساخته می‌شود. در فاز جانشینی، تصویر به سه کانال رنگ تقسیم می‌شود و در مرحله اول سطرهای هر کانال رنگ با یک کلید متفاوت رمزنگاری می‌شوند. در مرحله دوم ستون‌های هر سه کانال رنگ با کلیدهای متفاوت از مرحله قبل رمزنگاری می‌شوند. همچنین در فاز جای‌گشت، از نگاشت آرنولد[10] برای درهم سازی موقعیت پیکسل‌ها استفاده می‌شود.

خلیل و همکارانش [۱۰] روشی برای رمزنگاری تصاویر رنگی یا خاکستری مطرح کردند. در این روش در هر دو فاز جانشینی و جای‌گشت از ترکیب نگاشت‌های آشوب استفاده‌شده است. ابتدا برای رمزنگاری تصویر رنگی، سه کانال رنگ تصویر جدا و تبدیل به یک بردار یک‌بعدی می‌شوند. در فاز جای‌گشت، از یک نگاشت دوبعدی پیشنهادشده sin-cosine استفاده می‌شود و یک دنباله شبه‌تصادفی با طول مشابه با بردار کانال رنگ تولید می‌شود. با فرض طول بردار N برای هر کانال رنگ، اعداد دنباله تصادفی به عددی بین ۰ تا N تبدیل می‌شوند و موقعیت هر پیکسل، متناظر با موقعیت جدیدش در دنباله تصادفی تغییر می‌کند. در فاز جانشینی از نگاشت یک‌بعدی ترکیب‌شده از دو نگاشت تنت[11] و لجستیک[12] استفاده می‌شود و دنباله‌ای هم طول با بردار پیکسل‌های درهم شده مرحله قبل ایجاد می‌شود و درنهایت با اعمال عملگر XOR تصویر رمز شده به دست می‌آید.

تنوع بالایی از نگاشت‌های آشوب وجود دارد که بر اساس ابعادشان و دنباله‌هایی که تولید می‌کنند در روش‌های مختلف مورداستفاده قرار می‌گیرند. به‌عنوان‌مثال، وانگ و همکارانش [۱۱] درروش پیشنهادی‌شان از یک نگاشت آشوب ۶ بعدی به همراه تکنیک دنباله‌های DNA استفاده کرده‌اند و یا درروش پیشنهادی ژو و همکارانش [۱۲] از چهار نگاشت آشوب متفاوت در فرآیند رمزنگاری استفاده‌شده است.

ژو و همکارانش [۱۳] روشی برای رمزنگاری تصاویر رنگی بر

[1] Steganography
[2] Cover-media
[3] Cryptography
[4] Permutation
[5] Substitution
[6] Chaotic functions
[7] Metaheuristic

[8] Lorenz system
[9] Chen system
[10] Arnold's cat map
[11] Tent map
[12] Logistic map

پایه مفهوم مربع لاتین و توابع آشوب معرفی کردند. در این روش ابتدا توسط نگاشت آشوب سه بعدی Sine، سه دنباله شبه‌تصادفی برای تولید مربع لاتین متعامد سه بعدی و ماتریس تطبیق تولید می‌شود. در مرحله دوم، تصویر اصلی توسط مربع لاتین ۳ بعدی و ماتریس منطبق جای‌گشت داده می‌شود. بدین صورت که هر صفحه از ماتریس جای‌گشت به شانزده قسمت تقسیم شده و شماره‌گذاری می‌شود. سپس، یک دنباله آشوب با ابعاد ۱ در ۱۶ باتوجه‌به سه دنباله از پیش تولید شده استخراج می‌شود. دنباله ۱۶تایی مرتب می‌شود و باتوجه‌به اندیس داریه‌ها قبل و بعد از مرتب سازی ۱۶ قسمت ماتریس جای‌گشت بایکدیگر جابجا می‌شوند. باتوجه‌به موقعیت جدید درایه‌های ماتریس جای‌گشت، تصویر اصلی درهم ریخته می‌شود و در آخرین مرحله با استفاده از شیفت چرخشی تصویر رمزنگاری تولید می‌شود.

ژانگ و همکارانش [۱۴] روشی مبتنی بر نگاشت آشوب و عملیات RNA ارائه دادند. این روش دارای سه مرحله اصلی است و در هر مرحله از دنباله‌های آشوب مجزایی استفاده می‌شود. بنابراین در اولین مرحله با استفاده از یک نگاشت آشوب ۶ بعدی به تعداد $(3 \times N \times N + 64) \times 6$ ماتریس آشوب ساخته می‌شود. از ماتریس‌های ساخته شده سه ماتریس S_1، S_2 و S_3 باتوجه‌به ابعاد موردنیاز در هر مرحله استخراج می‌شود. از ماتریس S_1 در اولین مرحله و به منظور جای‌گشت پیکسل‌ها استفاده می‌شود. ماتریس کانال رنگ و ماتریس S_1 به دو آرایه یک بعدی تبدیل می‌شوند. آرایه S_1 به صورت صعودی مرتب می‌شود و بر اساس اندیس‌ها قبل و بعد از مرتب سازی، درایه متناظر در آرایه کانال رنگ موقعیتش تغییر می‌کند. در مرحله دوم با استفاده از ماتریس S_2، مرحله جابه‌جایی انجام می‌شود. ماتریس کانال رنگ و ماتریس S_2 به صورت یک مکعب تغییر شکل می‌دهند. با استفاده از تکنیک زیگ‌زاگ که بر روی سه وجه مکعب انجام می‌شود پیکسل متناظر با درایه مکعب S_2 با استفاده از عملگر XOR رمز می‌شود. در آخرین مرحله پیکسل‌ها به صورت دودویی تبدیل می‌شوند و بر اساس بیت‌ها و چهار جدول کدون[1] RNA، پیکسل‌ها کدگذاری می‌شوند و تصویر رمز شده نهایی به دست می‌آید.

در روش‌های رمزنگاری تصویر که بر پایه چکیده تصویر هستند، ابتدا یک تابع چکیده ساز بر روی تصویر ورودی اعمال می‌شود و یک‌رشته خروجی با طول ثابت ایجاد می‌کند که از رشته تولیدشده می‌توان در مرحله پردازش کلید رمزنگاری، به‌دست‌آوردن مقادیر اولیه نگاشت آشوب و... استفاده کرد. طول ثابت رشته خروجی و حساس‌بودن خروجی به تغییر یک بیت در تصویر ورودی، از مزایای استفاده چکیده تصویر در رمزنگاری تصویر است [۱۵, ۱۶].

در روشی که توسط زارعی [۱۷] ارائه‌شده است از ترکیب دو تابع چکیده ساز MD5 و SHA-256 برای ساخت کلید ۲۵۶ بیتی رمزنگاری استفاده‌شده است. در این روش اطلاعات تصویر اصلی و یک کلید ۲۵۶ بیتی تصادفی با استفاده از توابع چکیده ساز درهم می‌شوند و یک کلید ۲۵۶ بیتی محرمانه را نتیجه می‌دهند که در فرآیند تولید دنباله‌های آشوب و رمزنگاری مورداستفاده قرار می‌گیرد.

ژانگ و همکارش [۱۸] روشی برای رمزنگاری تصاویر رنگی معرفی کردند. در این روش از چکیده تصویر، نگاشت‌های آشوب و دنباله‌های DNA استفاده شده است. در اولین مرحله برای تولید کلید، ابتدا چکیده تصویر اصلی محاسبه می‌شود. از چکیده تصویر در مقداردهی اولیه نگاشت‌های آشوب و تنظیم پارامترها استفاده می‌شود. برای تولید چکیده تصویر، ابتدا تصویر اصلی به یک تصویر سطح خاکستری تبدیل می‌شود. سپس یک ماتریس چکیده تصویر با ابعاد برابر با تصویر خاکستری ساخته می‌شود. هر دو ماتریس دارای ابعاد ۲۵۶ در ۲۵۶ هستند. درایه‌های ماتریس چکیده بدین صورت مقداردهی می‌شوند که اگر درایه $i+1$ ماتریس خاکستری از درایه i ام کوچکتر باشد، درایه متناظر در ماتریس چکیده مقدار ۱ قرار می‌گیرد، در غیر این صورت مقدار درایه صفر خواهد بود. سپس ماتریس چکیده به ابعاد ۴۰۹۶ در ۱۶ تغییر شکل می‌دهد. از ماتریس جدید ۱۶ مقدار به دست می‌آید که ۹ مقدار به صورت تصادفی انتخاب می‌شوند. در مرحله بعد که مرحله جای‌گشت است، تصویر به سه کانال رنگ مجزا تقسیم می‌شود. با استفاده از یک نگاشت آشوب دوبعدی و مقادیر به دست آمده از مرحله قبل، به ازای هر کانال رنگ دو دنباله شبه‌تصادفی X و Y ساخته می‌شود. هر دو دنباله به صورت صعودی مرتب می‌شوند و بر اساس اندیس دنباله، قبل و بعد از مرتب سازی سطرها و ستون‌های کانال‌های رنگ جای‌گشت داده می‌شوند.

در آخرین مرحله یعنی جابه‌جایی، ۶ دنباله شبه‌تصادفی توسط یک نگاشت آشوب ۶ بعدی ساخته می‌شود. سه دنباله به طور تصادفی انتخاب می‌شوند و مقادیرشان به بازه ۰ تا ۲۵۵ نگاشت می‌شود. از دو دنباله دیگر برای انتخاب قانون کدگذاری DNA، و از دنباله آخر برای انتخاب نوع عملیات حسابی DNA استفاده می‌شود. در نهایت تصویر باتوجه‌به قوانین و عملگرهای انتخابی کدگذاری شده و تصویر رمز شده نهایی حاصل می‌شود.

ژو و همکارانش [۱۹] روشی به منظور رمزنگاری تصویر ارائه دادند که سعی شده است تا امنیت سیستم‌های رمزنگاری که از یک نگاشت آشوب استفاده می‌کنند بهبود ببخشد. در این روش از نگاشت آشوب یک‌بعدی لجستیک استفاده‌شده است و مقدار اولیه نگاشت با استفاده از چکیده تصویر که با الگوریتم SHA-512 به‌دست‌آمده است، محاسبه می‌شود. سپس با استفاده از

[1] Codons

دنباله شبه‌تصادفی تولیدشده و الگوریتم خوشه‌بندی K-mediods، مرحله جای‌گشت تصویر انجام می‌شود. در مرحله جانشینی، تصویر به‌هم‌ریخته مرحله قبل، با استفاده از دنباله شبه‌تصادفی و عملگر XOR رمزنگاری می‌شود.

الگوریتم‌های فراابتکاری، الگوریتم‌های تکرارشونده‌ای هستند که در هر مرحله باتوجه‌به اطلاعاتی که از وضعیت فعلی مسئله دریافت می‌کنند، قادر خواهند بود مؤلفه‌های هدف مسئله را بهبود ببخشند [۲۰]. از الگوریتم‌های فراابتکاری به دلیل ماهیتشان در بهینه‌سازی، می‌توان در بهبود عملکرد فرآیند رمزنگاری استفاده کرد [۲۱, ۲۲].

عبدالله و همکارانش [۲۳] روشی برای رمزنگاری تصویر مطرح کردند که برای اولین بار از الگوریتم ژنتیک[1] در رمزنگاری تصویر استفاده شد. برای مقداردهی اولیه جمعیت ابتدا تصویر به چهار قسمت تقسیم می‌شود. سپس از نگاشت آشوب لجستیک برای رمزنگاری پیکسل‌های هر قسمت استفاده می‌شود. پس از رمزنگاری تصویر الگوریتم ژنتیک اعمال می‌شود تا درنهایت بهترین تصویر رمز شده انتخاب گردد. به این منظور از عملگر همبری[2] استفاده می‌شود و قسمت‌های تصویر با یکدیگر جابجا می‌شوند تا شرط تابع هدف[3] مسئله که کمینه کردن همبستگی[4] بین پیکسل‌ها است برآورده شود.

ژانگ و همکارانش [۲۴] روشی بر پایه سیستم آشوب 2DNLCML[5] و عملگرهای الگوریتم ژنیتک برای رمزنگاری تصاویر رنگی ارائه دادند. ابتدا مقادیر اولیه سیستم 2DNLCML، توسط نگاشت آشوب لجستیک تولید می‌شود. سپس سیستم 2DNLCML به اندازه ابعاد تصویر یعنی $M \times N$ تکرار می‌شود تا دنباله شبه‌تصادفی ساخته شود. در ادامه کانال‌های رنگ تصویر اصلی جدا می‌شوند و هر کانال رنگ به یک آرایه یک بعدی تبدیل می‌شود.

در مرحله بعد پیکسل‌های هر کانال با استفاده دنباله شبه‌تصادفی و عملگر XOR رمزنگاری می‌شود. در مرحله بعد باتوجه‌به مقدار درایه دنباله آشوب متناظر با پیکسلی که در مرحله قبل رمز شده است، عملیات جهش انجام می‌شود. بدین صورت که اگر مقدار درایه دنباله آشوب زوج باشد جهش Inversion، و اگر فرد باشد جهش Swap بر روی پیکسل اعمال می‌شود.

در آخرین مرحله عملیات همبری دونقطه‌ای انجام می‌شود. به این صورت که همبری ابتدا برای پیکسل‌های جفت کانال‌های قرمز و سبز، و بعد از آن برای جفت کانال‌های آبی و قرمز اعمال می‌شود. نقاط همبری با استفاده از مقادیر دنباله آشوب تولید شده، انتخاب می‌شوند. بسته به تعداد دورهای موردنیاز برای الگوریتم رمزنگاری مراحل ذکر شده تکرار می‌شوند و تصویر رمز شده حاصل می‌شود.

چای و همکارانش [۲۵] روشی ترکیبی بر پایه عملگرهای الگوریتم ژنتیک، ماتریس تنسور، نگاشت آشوب و دنباله‌های DNA به منظور رمزنگاری تصویر ارائه دادند. ابتدا توسط یک نگاشت آشوب ۶ بعدی، شش دنباله شبه‌تصادفی ساخته می‌شود. دو دنباله‌ی دیگر یعنی دنباله هفتم و هشتم با استفاده از شش دنباله قبل و عملگرهای جمع و تفریق تولید می‌شوند. از هشت دنباله تولید شده در مراحل مختلف رمزنگاری استفاده می‌شود.

در ادامه، تصویر اصلی به اجزای قرمز، سبز و آبی خود تقسیم می‌شود و هر کانال رنگ به چهار قسمت مساوی تقسیم می‌شود. یک ماتریس با استفاده از مقادیر یکی از هشت دنباله که به‌صورت تصادفی انتخاب می‌شود، ساخته می‌شود. اولین بلاک تصویر با استفاده از عملیات ضرب تنسور در ماتریس ساخته شده، ضرب می‌شود. بلاک جدید به‌صورت ساعت‌گرد با دیگر بلاک‌ها XOR می‌شود و کانال رنگ رمز شده حاصل می‌شود.

عملیات XOR بین دو کانال رنگ دیگر نیز انجام می‌شود تا سه کانال رنگ رمز شده حاصل شود. سپس با استفاده از اولین و دومین دنباله شبه‌تصادفی و قوانین کدگذاری DNA، تصویر کدگذاری می‌شود. در ادامه عملیات همبری و جهش به ترتیب توسط دنباله‌های سوم تا پنجم و ششم تا هشتم انجام می‌شود.

در نهایت کدگشایی DNA انجام می‌شود و تصویر رمز شده نهایی به دست می‌آید. انتخاب پارامترهای همبری ژنتیکی، تعیین نقاط تقاطع، موقعیت و قاعده جهش توسط اطلاعات تصویر اصلی و توالی‌های آشوبی کنترل می‌شوند. البته انجام عملیات ضرب تنسورها وقت‌گیر خواهد بود، بنابراین ممکن است روش ارائه شده برای کاربردهای بلادرنگ مناسب نباشد.

سعید خان و همکاران [۲۶] روشی مطرح کردند که در آن از الگوریتم PSO[6] به‌منظور ساخت یک S-Box با خاصیت غیرخطی بودن استفاده کردند. برای ساخت S-Box، ابتدا جمعیت اولیه الگوریتم PSO به‌صورت تصادفی مقداردهی می‌شود. سپس در هر مرحله با استفاده از موقعیت عامل‌های الگوریتم PSO یک S-Box ساخته می‌شود و توسط معیارهایی که غیرخطی بودن را بررسی می‌کنند ارزیابی می‌شود. درنهایت S-Box که خاصیت غیرخطی بالایی دارد انتخاب، و در مرحله جای‌گشت استفاده می‌شود.

همان‌طور که اشاره شد، برای تأمین امنیت داده‌ها استفاده از الگوریتم‌های رمزنگاری امری اجتناب‌ناپذیر است، اما مدیریت

[1] Genetic algorithm
[2] Crossover
[3] Fitness function
[4] Correlation
[5] Two Dimensional Nonlinear Coupled Map Lattices
[6] Particle swarm optimization

کلید رمزنگاری مسئله‌ای جدی و مهم است. در اکثر روش‌های ارائه‌شده در رمزنگاری تصویر، کلید رمزنگاری با استفاده از پارامترهای نگاشت آشوب، اطلاعات تصویر و... تولید می‌شود. برای افزایش امنیت رمزنگاری، می‌توان از مؤلفه‌های بیومتریک[1] در تولید کلید استفاده کرد و جهت ذخیره‌سازی ایمن کلید می‌توان از زنجیره‌بلوکی[2] بهره گرفت.

ژاو و همکارانش [۲۷] روشی برای رمزنگاری تصویر و احراز هویت[3] و صحت فرد فرستنده (رمزنگار) و گیرنده بر بستر زنجیره‌بلوکی معرفی کردند. در شبکه زنجیره‌بلوکی طراحی‌شده به هر کاربر (فرستنده یا گیرنده) یک شناسه منحصربه‌فرد که کلید عمومی است تعلق می‌گیرد. هر تراکنش شبکه زنجیره‌بلوکی شامل یک امضا خاص است که از چکیده تصویر رمز شده، کلید عمومی فرستنده، کلید عمومی گیرنده و کلید رمزنگاری با استفاده از الگوریتم SHA-256 حاصل می‌شود. در این سیستم فرستنده تصویر رمز شده را به همراه امضا بر روی شبکه ارسال می‌کند و پس از تأیید تراکنش توسط گره‌های شبکه، گیرنده می‌تواند درخواست خود را برای دریافت تصویر رمز شده ارسال کند و پس از احراز هویت و دریافت اطلاعات موردنیاز، رمزگشایی را انجام دهد.

لی و همکارانش [۲۸] یک روش رمزنگاری تصویر مبتنی برنگاشت آشوب و اثرانگشت بر بستر زنجیره‌بلوکی را ارائه کردند. در این روش کلید رمزنگاری با استفاده از اطلاعات اثرانگشت به دست می‌آید. همچنین اطلاعات اثرانگشت در تصویر رمزنگاری شده ثبت‌شده و انتقال تصاویر بین فرستنده و گیرنده بر بستر زنجیره‌بلوکی انجام می‌شود؛ بنابراین می‌توان از صحت هویت فرستنده و گیرنده اطمینان حاصل کرد.

در ادامه ساختار مقاله بدین صورت خواهد بود که در بخش دوم الگوریتم ژنتیک، توابع آشوب آرنولد و لورنز معرفی می‌شوند. سپس روشی که به‌منظور شناسایی و کدگذاری چهره استفاده شده است بررسی می‌شود. در بخش سوم، روش پیشنهادی با دید پایین‌به‌بالا شرح داده می‌شود. بدین معنا که ابتدا قسمت‌های جزئی سیستم بررسی می‌شود و سپس یک سیستم کامل برای رمزنگاری تصویر ارائه می‌شود. در بخش چهارم ابتدا معیارهای سنجش یک الگوریتم رمزنگاری تصویر معرفی می‌شوند و سپس با استفاده از جداول، نمودارها و تصاویر نتایج الگوریتم پیشنهادی بررسی می‌شود. همچنین نتایج روش پیشنهادی با سایر روش‌های ارائه شده مشابه مقایسه می‌شود تا کارایی الگوریتم پیشنهادی بررسی شود. در بخش پنجم نتیجه‌گیری تحقیق انجام شده بیان شده است.

۲- ۲- مفاهیم مقدماتی

در این بخش تکنیک‌ها و الگوریتم‌های استفاده‌شده درروش پیشنهادی معرفی می‌شوند. این بخش شامل معرفی نگاشت‌های آشوب لورنز و آرنولد، الگوریتم فراابتکاری ژنتیک و الگوریتم استخراج ویژگی‌های چهره است.

۲-۱- ۲-۱ نگاشت آشوب

نظریه آشوب شاخه‌ای از ریاضیات است که به بررسی رفتار آن دسته از سیستم‌های دینامیکی غیرخطی می‌پردازد که به شرایط اولیه بسیار حساس هستند [۲۹].

دنباله اعداد تولیدشده توسط نگاشت‌های آشوب در ظاهر تصادفی و بدون نظم و ترتیب هستند؛ اما در عمل وابسته به قوانین، الگوهای خاص و شرایط اولیه سیستم هستند. تاکنون نگاشت‌های آشوب متنوعی مانند لجستیک، استاندارد، آرنولد، هنون[4]، لورنز و... ارائه‌شده‌اند که هرکدام باتوجه‌به مؤلفه‌هایی مانند ابعاد نگاشت آشوب، تعداد پارامترها و رفتاری که نگاشت آشوب از خود نشان می‌دهد در کاربردهای مختلف استفاده می‌شوند.

۲-۲- ۲-۲ نگاشت آرنولد

نگاشت آرنولد در سال ۱۹۶۰ توسط ولادیمر آرنولد[5] معرفی شد. نگاشت آرنولد یک نگاشت دوبعدی است که طبق رابطه (۱) تعریف می‌شود [۳۰].

$$C = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \det C = 1$$
$$\begin{bmatrix} x' \\ y' \end{bmatrix} = C \begin{bmatrix} x \\ y \end{bmatrix} mod\ 1 \quad (۱)$$

که x و y موقعیت فعلی یک نقطه، x' و y' موقعیت جدید نقطه در فضای دوبعدی را نشان می‌دهند. و C یک ماتریس وارون‌پذیر است.

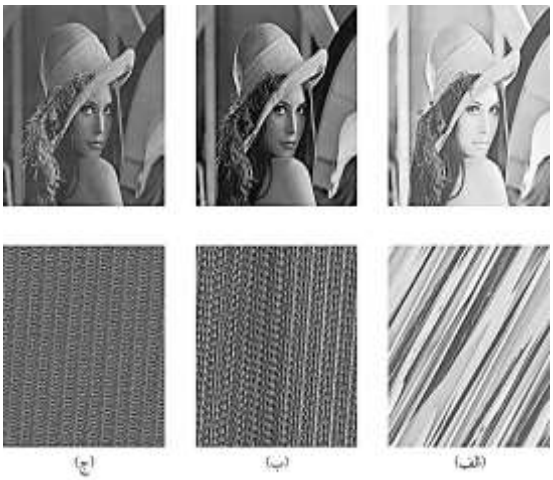
در فرآیند رمزنگاری تصویر می‌توان از نگاشت آرنولد به‌منظور به‌هم‌ریختن موقعیت پیکسل‌های تصویر استفاده کرد. برای این منظور، ابتدا ماتریس ثابت C در رابطه (۱) به شکل ماتریس C در رابطه (۲) به دلیل افزایش ضریب امنیت و خاصیت تصادفی بودن بازنویسی می‌شود که با اعمال این رابطه بر روی ماتریس دوبعدی تصویر، موقعیت پیکسل‌ها تغییر می‌کند [۳۱].

$$C = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}; \det C = 1;\ p, q \geq 0$$
$$\begin{bmatrix} x' \\ y' \end{bmatrix} = C \begin{bmatrix} x \\ y \end{bmatrix} mod\ N \quad (۲)$$

[1] Biometrics
[2] Blockchain
[3] Authentication
[4] Hénon map
[5] Vladimir Arnold

که x و y موقعیت فعلی یک پیکسل، x' و y' موقعیت جدید پیکسل در ماتریس دوبعدی تصویر و N ابعاد تصویر (با فرض مربعی بودن تصویر) را نشان می‌دهند.

به‌عنوان‌مثال، سه کانال رنگ آبی، سبز و قرمز تصویر لنا جداسازی شده و پیکسل‌های هر سه کانال رنگ به‌ازای پارامترهای مختلف جابه‌جا شده‌اند. برای کانال آبی پارامترهای $p = 12$ و $q = 71$ برای کانال سبز پارامترهای $p = 10$ و $q = 3$ و کانال قرمز پارامترهای $p = 1$ و $q = 2$ استفاده‌شده است. نتایج جابه‌جایی پیکسل‌های هر سه کانال رنگ در شکل (۱) نشان داده‌شده است.



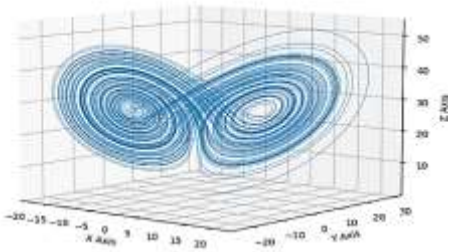
شکل (۱). اعمال نگاشت آشوب آرنولد بر روی سه کانال رنگ تصویر لنا. الف: کانال رنگ قرمز به ازای پارامترهای $p = 1$ و $q = 2$. ب: کانال رنگ سبز به ازای پارامترهای $p = 10$ و $q = 3$. ج: کانال رنگ آبی به ازای پارامترهای $p = 12$ و $q = 71$.

۲-۳- ۲-۳ نگاشت لورنز

سیستم لورنز یک سیستم دیفرانسیل معمولی، غیرخطی و سه‌بعدی است که در سال ۱۹۶۳ توسط ادوارد لورنز[1] به‌منظور مدل‌سازی ریاضی همرفت جوی معرفی شد [۳۲]. سیستم لورنز استاندارد، دارای سه پارامتر σ، ρ و β هستند که به‌صورت رابطه (۳) معرفی می‌شود.

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \quad (۳)$$

که σ، ρ و β مقادیر مثبت هستند که به ترتیب به ازای مقادیر ۱۰، ۲۸ و $\frac{۸}{۳}$ سیستم رفتار آشوبناک نشان خواهد داد. $x_0 = 0.27$، $y_0 = 1.0$ و $z_0 = 0.63$ توابعی برحسب زمان هستند که مقادیر جدید را بر اساس مقادیر قبلی دنباله تولید می‌کنند. در شکل (۲) مثالی از رفتار سیستم لورنز به ازای مقادیر اولیه $x_0 = 0.27$، $y_0 = 1.0$ و $z_0 = 0.63$ و پارامترهای ذکرشده در ۱۰۰۰۰ تکرار نشان داده‌شده است.



شکل (۲). مثالی از رفتار نگاشت آشوب لورنز به ازای مقادیر اولیه $x_0 = 0.27$، $y_0 = 1.0$ و $z_0 = 0.63$ و پارامترهای $\sigma = 10$، $\rho = 28$ و $\beta = \frac{8}{3}$

۲-۴- ۲-۴ الگوریتم ژنتیک

الگوریتم ژنتیک، یک روش جستجو و بهینه‌سازی بر اساس اصول تکامل طبیعی است [۳۳]. این الگوریتم جزء الگوریتم‌های تکاملی قرار می‌گیرد که بر اساس تئوری تکامل انتخاب طبیعی داروین پایه‌گذاری شده است. در این الگوریتم‌ها، یک جمعیت از طریق انتخاب اعضای برتر و کنار گذاشتن اعضای پست‌تر در طی فرآیند تولیدمثل و تکامل، بهبود می‌یابد. الگوریتم ژنتیک اجازه می‌دهد که یک جمعیت متشکل از تعداد زیادی افراد که تحت قوانین ویژه‌ای تشکیل‌شده‌اند، در طی فرآیند تکامل تابع هدف را بهینه نمایند. الگوریتم ژنتیک با ایجاد یک جمعیت اولیه از کروموزوم‌ها[2] آغاز می‌شود. به‌عبارتی‌دیگر کروموزوم‌ها، رشته‌هایی از مقادیر پیشنهادی برای متغیرهای تصمیم مسئله هستند و هر یک نمایانگر یک پاسخ محتمل برای مسئله هستند. در مرحله بعد، کروموزوم‌ها باتوجه‌به هدف بهینه‌سازی مورد ارزیابی قرار می‌گیرند و کروموزوم‌هایی که پاسخ‌های بهتری برای مسئله موردنظر محسوب می‌شوند، شانس بیشتری برای تولید مجدد جواب‌های مسئله پیدا می‌کنند.

در مرحله تولیدمثل سه عملگر مهم و کلیدی وجود دارد: ۱) عملگر انتخاب: با استفاده از این عملگر از بین کروموزوم‌های موجود در جمعیت تعدادی برای تولیدمثل انتخاب می‌شوند. انتخاب کروموزوم‌ها به‌صورت تصادفی اتفاق می‌افتد اما باید به‌گونه‌ای باشد که کروموزوم‌هایی که شایستگی بیشتر دارند، احتمال بیشتری برای انتخاب داشته باشند. ۲) عملگر همبری: این عملگر بر روی دو یا چند والد اعمال می‌شود و با ادغام و یا تعویض برخی از ژن‌ها دو یا چند فرزند تولید می‌شود. ۳) عملگر جهش[3]: این عملگر یک یا چند ژن را به‌صورت تصادفی تغییر می‌دهد.

۲-۵- ۲-۵ استخراج ویژگی‌های چهره

[1] Edward Norton Lorenz

[2] Chromosome
[3] Mutation

استفاده از ویژگی‌های بیومتریک در فرآیند تولید کلید و احراز هویت اولین‌بار در سال ۱۹۹۴ مطرح شد [۳۴]. در این‌گونه روش‌ها می‌توان از ویژگی‌هایی مانند چهره، اثرانگشت، قرنیه، صوت و ... استفاده کرد که به دلیل منحصربه‌فرد بودن اطلاعات نسبت به سایر افراد، و عدم نیاز به نگهداری امن این ویژگی‌ها در بسیاری از کاربردهای رمزنگاری و احراز هویت استفاده می‌شوند [۳۵]. ویژگی‌های چهره یک فرد شامل اطلاعاتی است که در قالب برداری با مقادیر عددی شناخته می‌شود. هرکدام از مقادیر این بردار یک ویژگی را بیان می‌کند، مانند فاصله بین دو چشم، طول ابرو، فاصله بین لب تا چانه و... که برای هر فرد منحصربه‌فرد خواهد بود. استخراج ویژگی‌های چهره به‌صورت کلی در دو مرحله انجام می‌شود [۳۶]: ۱) شناسایی چهره[1] ۲) کدگذاری چهره[2].

۱) شناسایی چهره: در این مرحله قسمتی از تصویر که چهره فرد را شامل می‌شود شناسایی می‌شود که می‌توان از الگوریتم‌های متنوعی مانند HOG، MTCNN و SVM استفاده کرد [۳۷–۳۹].

۲) کدگذاری چهره: به‌منظور کدگذاری چهره می‌توان از شبکه‌های عصبی کانولوشن[3] استفاده کرد. شبکه FaceNet در سال ۲۰۱۵ توسط محققان گوگل معرفی شد [۴۰]. آموزش این شبکه بر روی‌داده‌های LFW[4] انجام‌شده و دقت تشخیص این مدل ۹۹/۶۳ درصد است. این روش به دلیل دقت بالاتر نسبت به روش‌هایی مانند VGG-Face و DeepID که به ترتیب دارای ۹۷/۷۸ و ۹۹/۱۵ درصد هستند در کاربردهای بیشتری استفاده می‌شود. خروجی این شبکه یک بردار عددی ۱۲۸ تایی است که هر مؤلفه از آن نشان‌دهنده‌ی یک ویژگی چهره است.

۳- ۳- روش پیشنهادی

در این بخش روش پیشنهادی رمزنگاری تصویر بیان می‌شود. کلید رمزنگاری با استفاده از اطلاعات چهره کاربر، کلید عمومی و تصویر اصلی ساخته می‌شود. در فاز جانشینی پیکسل‌ها هر قسمت از تصویر با استفاده از یک دنباله شبه‌تصادفی جداگانه رمزنگاری می‌شود. در فاز جای‌گشت، به‌وسیلهٔ الگوریتم ژنتیک یک حالت بهینه برای به‌هم‌ریختن پیکسل‌ها انتخاب می‌شود تا همبستگی بین پیکسل‌ها به طور مناسبی کاهش یابد.

۳-۱- ۳-۱ چکیده تصویر

محاسبه چکیده تصویر به‌وسیلهٔ الگوریتم SHA-512 انجام می‌شود. برای محاسبه چکیده تصویر، ابتدا مقادیر پیکسل‌های هر سه کانال رنگ (در تصاویر خاکستری یک کانال رنگ) به رشته‌ای از بایت‌ها تبدیل می‌شود و به‌عنوان ورودی به تابع محاسبه چکیده اعمال می‌شود و یک خروجی ۵۱۲ بیتی که متأثر از تمام پیکسل‌های تصویر است را نتیجه می‌دهد.

۳-۲- ۳-۲ کلید عمومی و خصوصی

از جفت کلیدهای عمومی و خصوصی در فرآیند رمزگشایی و احراز هویت استفاده می‌شود. درروش پیشنهادی از کلیدهای ۱۰۲۴ بیتی که توسط الگوریتم RSA تولید می‌شوند استفاده می‌شود.

۳-۳- ۳-۳ بردار ویژگی‌های چهره

اطلاعات چهره فرد رمزگذار با استفاده از الگوریتم‌های معرفی‌شده در بخش ۲-۵ استخراج و کدگذاری می‌شوند؛ و خروجی نهایی یک بردار است که دارای ۱۲۸ درایه اعشاری است و هر درایه نشان‌دهنده یک یا ترکیبی از چند ویژگی چهره مانند فاصله دو چشم، طول لب‌ها و... است.

۳-۴- ۳-۴ مقادیر اولیه نگاشت لورنز

همان‌طور که در بخش ۲-۳ نگاشت لورنز بررسی شد، این نگاشت به سه مقدار اولیه نیاز خواهد داشت. درروش پیشنهادی ابتدا تصویر همانند شکل (۳) به چهار قسمت تقسیم می‌شود سپس به ازای هر قسمت سه دنباله آشوب برای رمزنگاری سه کانال رنگ تولید می‌شود؛ بنابراین به ۱۲ دنباله آشوب نیاز است که به این منظور باید ۱۲ مقدار اولیه مشخص شوند.

برای تولید مقادیر اولیه نگاشت، ابتدا توسط الگوریتم SHA-512 چکیده سه داده، چکیده تصویر، بردار ویژگی‌های چهره و کلید عمومی محاسبه می‌شود. رشته ۵۱۲ بیتی نهایی به چهار قسمت مساوی ۱۲۸ بیتی تقسیم می‌شود. در مرحله بعد هر قسمت ۱۲۸ بیتی به سه رشته ۴۰ بیتی تقسیم می‌شود. در اینجا از ۸ بیت کم ارزش هر کدام از رشته‌های ۱۲۸ بیتی صرف نظر می‌شود. سپس بیت‌های هرکدام از رشته‌های ۴۰ بیتی دوبه‌دو (بیت‌های مجاور) با یکدیگر XOR می‌شوند. در آخرین مرحله سه بردار ۳۹ بیتی دودویی به سه عدد ده‌دهی تبدیل می‌شوند.

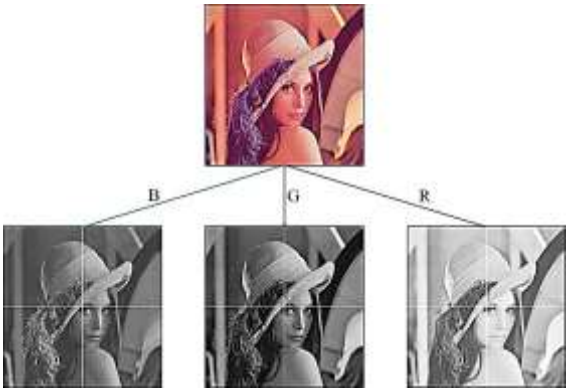
سه عدد به‌دست‌آمده طبق رابطه (۴) به سه عدد بین ۰ و ۱ تبدیل خواهند شد. با تکرار مراحل ذکرشده برای ۴ قسمت تصویر و هر سه کانال رنگ، ۱۲ مقدار اولیه بین ۰ و ۱ برای نگاشت آشوب لورنز به دست می‌آید.

$$x_i, y_i, z_i = \frac{b2d(\vec{x}) \,\%\, 2^8}{2^8} \qquad (۴)$$

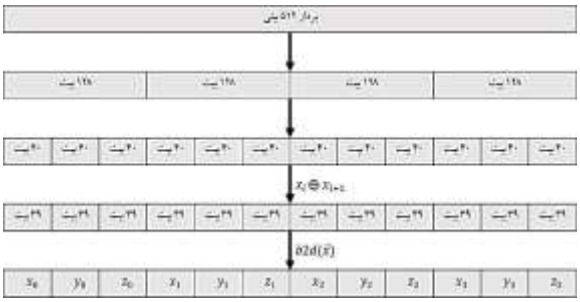
که در رابطه (۴)، $\vec{x}$ بردار ۳۹ بیتی، $b2d()$ تابعی برای تبدیل عدد دودویی به عددی ده‌دهی و $\%$ عملگر محاسبه باقی‌مانده تقسیم است؛ بنابراین مقادیر اولیه نگاشت متأثر از کلید عمومی، ویژگی‌های چهره و مقادیر پیکسل‌های هر سه کانال رنگ

[1] Face detection
[2] Face encoding
[3] Convolutional neural network
[4] Labeled Faces in the Wild

خواهد بود. مراحل محاسبه مقادیر اولیه نگاشت آشوب در شکل (۴) نشان داده‌شده است.



شکل (۳). جداسازی کانال‌های رنگ تصویر لنا و تقسیم‌بندی هر کانال رنگ به چهار قسمت مساوی



شکل (۴). مراحل محاسبه دوازده مقدار اولیه برای نگاشت آشوب لورنز

۳-۵- ۵-۳ تولید دنباله‌های شبه‌تصادفی

با استفاده از ۱۲ مقدار اولیه تولیدشده در بخش ۳-۴، ۱۲ دنباله شبه‌تصادفی تولید می‌شود. برای تولید دنباله از نگاشت آشوب لورنز با پارامترهای معرفی‌شده در بخش ۲-۳ استفاده می‌شود. ابتدا سه دنباله S_{01}، S_{02} و S_{03} با استفاده از سه مقدار اولیه x_0، y_0 و z_0 تولید می‌شوند. سپس سه دنباله S_{11}، S_{12} و S_{13} با استفاده از سه مقدار اولیه x_1، y_1 و z_1 تولید می‌شوند. به طور مشابه طبق رابطه (۵)، دوازده دنباله شبه‌تصادفی تولید می‌شوند.

$$\begin{aligned} S_{01}, S_{02}, S_{03} &= Lorenz\_System(x_0, y_0, z_0) \\ S_{11}, S_{12}, S_{13} &= Lorenz\_System(x_1, y_1, z_1) \\ S_{21}, S_{22}, S_{23} &= Lorenz\_System(x_2, y_2, z_2) \\ S_{31}, S_{32}, S_{33} &= Lorenz\_System(x_3, y_3, z_3) \end{aligned} \quad (۵)$$

که در رابطه (۵)، $Lorenz\_System(x_i, y_i, z_i)$ تابعی است برای تولید سه دنباله شبه‌تصادفی با استفاده سه مقدار اولیه ورودی و S_{ij} j امین دنباله تولیدشده با استفاده از i امین دسته مقادیر اولیه است. درروش پیشنهادی طول دنباله‌های تولیدشده با یکدیگر برابر، و برابر با تعداد پیکسل‌های یکی از چهار قسمت تصویر است بنابراین اگر تصویر اصلی N سطر و M ستون داشته باشد و چهار قسمت مساوی تقسیم شود، طول هر دنباله $M / 4 \times N / 4$ خواهد بود.

۳-۶- ۶-۳ الگوریتم رمزنگاری

الگوریتم رمزنگاری پیشنهادی دارای دوفاز اصلی جانشینی (تغییر مقادیر پیکسل‌ها) و جای‌گشت (تغییر موقعیت پیکسل‌ها) است که در شکل (۵) نشان داده‌شده است. همچنین الگوریتم رمزنگاری و رمزگشایی مشابه هستند و تنها در برخی از پارامترهای ورودی متفاوت هستند. درروش پیشنهادی هر کانال رنگ به طور جداگانه رمزنگاری می‌شود. الگوریتم رمزنگاری شامل ۴ مرحله زیر است:

مرحله اول: استخراج ویژگی‌های بیومتریک چهره و محاسبه چکیده تصویر.

مرحله دوم: محاسبه ۱۲ مقدار اولیه نگاشت آشوب لورنز.

مرحله سوم: در این مرحله فاز جانشینی پیکسل‌ها انجام می‌شود. هرکدام از کانال‌های رنگ به چهار قسمت تقسیم می‌شوند و هرکدام از قسمت‌ها، با استفاده از یکی از دنباله‌های S_{ij} تولیدشده در بخش ۳-۵ رمزنگاری می‌شوند. برای رمزنگاری سه حالت در نظر گرفته می‌شود. اگر کانال رنگ قرمز باشد قسمت‌های اول تا چهارم این کانال به ترتیب با استفاده از دنباله‌های S_{01}، S_{11}، S_{21} و S_{31} و اگر کانال رنگ سبز باشد قسمت‌های اول تا چهارم این کانال به ترتیب با استفاده از دنباله‌های S_{02}، S_{12}، S_{22} و S_{32} و اگر کانال رنگ آبی باشد قسمت‌های اول تا چهارم این کانال به ترتیب با استفاده از دنباله‌های S_{03}، S_{13}، S_{23} و S_{33} با استفاده از رابطه‌ی (۶) رمزنگاری می‌شوند.

$$Pix_{New} = [Pix_{Old} \oplus round\,(S_{ij} \times 255)]\%256 \quad (۶)$$

که Pix_{New} مقدار جدید پیکسل، Pix_{Old} مقدار فعلی پیکسل، S_{ij} دنباله شبه‌تصادفی، $round$ عبارت ورودی را به نزدیک‌ترین عدد صحیح تبدیل می‌کند، $\oplus$ علامت XOR و $\%$ علامت محاسبه باقی‌مانده است. بنابراین هر چهار قسمت کانال‌های رنگ رمزنگاری می‌شوند. سپس چهار قسمت هر کانال مجدد کنار یکدیگر قرار می‌گیرند.

مرحله چهارم: در این مرحله فاز جای‌گشت انجام می‌شود و موقعیت پیکسل‌های رمز شده کانال‌های رنگ به‌دست‌آمده از مرحله قبل توسط نگاشت آرنولد که در بخش ۲-۲ معرفی شد، به‌هم‌ریخته می‌شوند. دو پارامتر اصلی a و b در نگاشت آرنولد به‌صورت ثابت تنظیم نمی‌شوند، بلکه توسط الگوریتم فرابتکاری ژنتیک بهینه‌ترین پارامترها انتخاب می‌شوند. به‌منظور انتخاب بهینه پارامترهای نگاشت آرنولد توسط الگوریتم فرابتکاری ژنتیک مراحل زیر طی می‌شوند:

الف) مقداردهی اولیه عامل‌ها: در این مرحله جمعیت الگوریتم بهینه‌سازی را مقادیر مختلف پارامترهای a و b می‌سازند. بنابراین مسئله دارای دو متغیر است. هرکدام از متغیرها

یک عدد صحیح مثبت هستند که در اینجا مقدار هر متغیر در بازه‌ی [۱،۶۵۵۳۵] قرار می‌گیرد؛ یعنی برای هر متغیر ۱۶ بیت در نظر گرفته می‌شود. به‌عنوان‌مثال اگر جمعیت دارای ۱۰۰ عضو باشد و هر عضو دارای دو متغیر باشد، بنابراین یک ماتریس ۱۰۰ ✕ ۳۲ به‌صورت تصادفی ساخته می‌شود.

ب) ارزیابی عامل‌ها: پس از ساخت جمعیت اولیه نوبت به ارزیابی عامل‌ها است تا شایسته‌ترین عامل مشخص شود. برای ارزیابی عامل‌ها، تابع شایستگی؛ همبستگی بین پیکسل‌های تصویر تعریف می‌شود؛ یعنی به‌ازای متغیرهای a و b یک عامل، پیکسل‌های تصویر توسط نگاشت آرنولد به‌هم‌ریخته می‌شوند. سپس مقدار همبستگی پیکسل‌های سطر، ستون و قطر ماتریس به‌هم‌ریخته شده اندازه‌گیری می‌شود؛ بنابراین بهینه‌سازی بر روی سه هدف به طور هم‌زمان باید انجام شود. ازاین‌رو مسئله چند هدفِ را با استفاده از روش مجموع وزن‌دار اهداف، به یک مسئله تک هدفِ تبدیل می‌کنیم؛ بنابراین سه مقدار اندازه‌گیری شده با وزن‌های یکسان با یکدیگر جمع می‌شوند تا یک عدد صحیح را نتیجه دهند. عدد به‌دست‌آمده نشان‌دهنده شایستگی آن عامل خواهد بود و هر چه این مقدار کمتر باشد، شایستگی عامل بیشتر خواهد بود؛ بنابراین بهینه‌سازی مسئله، کمینه‌سازی تابع هدف است.

ج) بروز رسانی جمعیت: عامل‌ها بر اساس شایستگی‌شان به‌روزرسانی می‌شوند و جمعیت مرحله بعد ساخته می‌شود (انتخاب، همبری، جهش).

د) پاسخ نهایی: درنهایت پس از رسیدن به‌شرط توقف مسئله که در اینجا تعداد تکرارهای الگوریتم فراابتکاری تنظیم‌شده است، بهترین مقادیر a و b برای نگاشت آرنولد انتخاب می‌شوند و جای‌گشت تصویر انجام می‌شود.

شکل (۵). شماتیک الگوریتم رمزنگاری پیشنهادی که دارای دو فاز اصلی جانشینی و جایگشت است.

۳-۷- ۷-۳ کلید رمزنگاری

کلید رمزنگاری و رمزگشایی یکسان خواهند بود. همچنین کلید باید دارای طول قابل‌قبولی برای تأمین امنیت باشد. کلید با استفاده از اطلاعاتی که در رمزنگاری استفاده‌شده است ساخته می‌شود. ابتدا رشته ۵۱۲ بیتی حاصل از چکیده کلید عمومی، ویژگی‌های چهره و چکیده تصویر نیاز است. همچنین نگاشت لورنز دارای سه پارامتر اعشاری است بنابراین برای هر پارامتر ۶۴ بیت در نظر گرفته می‌شود که درمجموع ۱۹۲ بیت نیاز خواهد داشت. آخرین قسمت کلید شامل پارامترهای نگاشت آرنولد خواهد بود که در فاز جای‌گشت تصویر استفاده‌شده‌اند. برای هر متغیر به ۱۶ بیت نیاز است که درمجموع برای ۶ متغیر در تصاویر رنگی (۲ متغیر به ازای هر کانال رنگ) و ۲ متغیر در تصاویر خاکستری به ترتیب ۹۶ و ۳۲ بیت نیاز است؛ بنابراین در تصاویر رنگی طول کلید ۸۰۰ بیت و در تصاویر خاکستری ۷۳۶ بیت خواهد بود. ترتیب قرارگیری اطلاعات و ساخت کلید این‌گونه خواهد بود که ابتدا رشته ۵۱۲ بیتی در سمت چپ، پس‌ازآن رشته ۱۹۲ بیتی و در آخر رشته ۹۶ بیتی یا ۳۲ بیتی بسته به نوع تصویر کنار یکدیگر قرار می‌گیرند.

۳-۸- ۸-۳ ذخیره کلید در زنجیره‌بلوکی

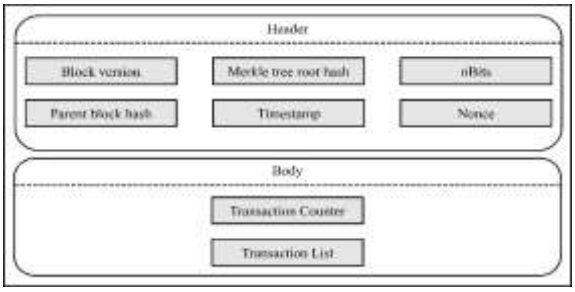
به‌منظور نگهداری ایمن کلید رمزنگاری و همچنین احراز هویت کاربر، پس از رمزنگاری تصویر، کلید تولیدشده در بخش ۳-۷ و بردار ویژگی‌های چهره کاربر در یک شبکه زنجیره‌بلوکی ذخیره‌سازی می‌شوند. در شبیه‌سازی زنجیره‌بلوکی روش پیشنهادی، از IPFS[1] مبتنی بر اتریوم[2] با استفاده از زبان برنامه‌نویسی Golang استفاده‌شده است. ساختار بلوک‌ها در شبکه در شکل (۶) نشان داده‌شده است. هر بلوک دارای دو قسمت اصلی تیتر[3] و بدنه[4] است. در قسمت تیتر؛ نسخه شبکه زنجیره‌بلوکی، مهر زمانی[5]، رشته Nonce، درجه سختی، چکیده بلوک قبل و ریشه درخت مرکل قرار می‌گیرد. در قسمت بدنه بلوک تراکنش‌ها قرار می‌گیرند، هر تراکنش به‌صورت رابطه (۷) تعریف می‌شود.

$$Transaction = Enc[(Face\ Vector, Key), Public\ Key] \quad (۷)$$

که $Enc[(x), Public\ Key]$ رمزنگاری داده x با استفاده

[1] InterPlanetary File System
[2] Ethereum
[3] Header
[4] Body
[5] Timestamp

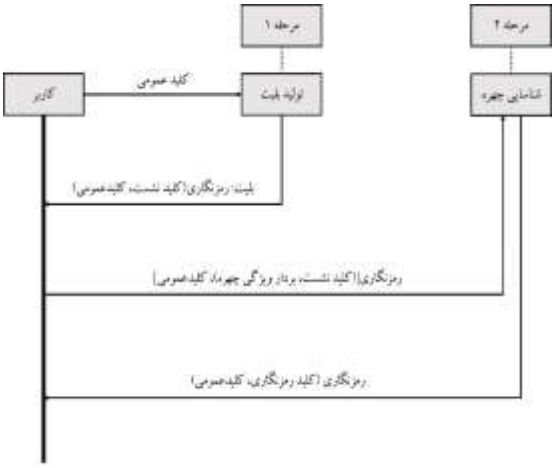
از الگوریتم RSA و کلید عمومی $Public\ Key$، بردار ویژگی‌های چهره و $Face\ Vector$ کلید Key ۸۰۰ بیتی (تصاویر رنگی) یا ۷۳۶ بیتی (تصاویر خاکستری) است.



شکل (۶). ساختار یک بلوک در زنجیره‌بلوکی

۳-۹- ۹-۳ رمزگشایی و احراز هویت

به‌منظور رمزگشایی تصاویر دو مرحله احراز هویت اجرا می‌شود. سیستم احراز هویت دومرحله‌ای روش پیشنهادی در شکل (۷) نشان‌داده‌شده است. در اولین مرحله کاربر برای رمزگشایی تصویر، کلید عمومی خود را به‌عنوان یک شناسه کاربری ارسال می‌کند. سیستم یک بلیت (پیام) که حاوی کلید موقت نشست است را با استفاده از کلید عمومی کاربر رمزنگاری و برای کاربر ارسال می‌کند. تنها، فردی می‌تواند به کلید نشست دسترسی پیدا کند که بتواند بلیت را با استفاده از کلید خصوصی‌اش رمزگشایی کند. همچنین ارائه بلیت برای رسیدن به مرحله دوم الزامی است. در مرحله دوم، تصویری از چهره فرد دریافت می‌شود. سپس بردار ویژگی‌های چهره استخراج می‌شود. ویژگی‌های چهرهٔ دریافتی با بردار ویژگی‌های چهره ذخیره‌شده در زنجیره‌بلوکی مطابق بخش ۳-۱۰ مطابقت داده می‌شوند. اگر تأیید شود که چهره فرد درخواست‌کننده با چهره فرد رمزنگار یکسان است (درخواست‌کننده همان فرد رمزگذار است) کلید موردنیاز رمزگشایی که در زنجیره‌بلوکی ذخیره‌شده است، برای کاربر ارسال می‌شود. پس از دریافت کلید رمزنگاری، فرآیند رمزگشایی معکوس رمزنگاری خواهد بود.



شکل (۷). احراز هویت دومرحله‌ای به‌منظور رمزگشایی تصویر

۳-۱۰- ۱۰-۳ تطابق چهره

به‌منظور مشخص‌کردن انطباق دو چهره کافی است که بردار ویژگی‌های دو چهره استخراج شوند. سپس فاصلهٔ بین دو بردار اندازه‌گیری شود. اگر فاصلهٔ بین دو بردار از یک حد آستانه بیشتر باشد انطباق دو چهره رد می‌شود؛ اما اگر فاصله از حد آستانه کمتر باشد، انطباق چهره‌ها تأیید می‌شود. برای اندازه‌گیری فاصله دو بردار از فاصله اقلیدسی استفاده می‌شود:

فاصله اقلیدسی: فاصله بردار ویژگی اول x و بردار ویژگی دوم y طبق رابطه (۸) محاسبه می‌شود.

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \qquad (۸)$$

که $i = 1,2,\dots,n$ اندیس ویژگی‌ها و n تعداد ویژگی‌ها است. مقادیر حد آستانه به‌صورت آزمایشی و تجربی به‌دست‌آمده‌اند که بسته به مدل یادگیری متفاوت هستند. مقادیر حد آستانه برای مدل FaceNet، برای فاصله‌های اقلیدسی و اقلیدسی نرمال شده، مقادیر ۱۰ و ۰/۸ هستند.

۴- ۴- ارزیابی و نتایج

برای بررسی عملکرد و کارایی یک الگوریتم رمزنگاری، نیاز است آزمایش‌هایی بر روی نتایج به‌دست‌آمده از آن الگوریتم صورت گیرد. در الگوریتم‌های رمزنگاری تصاویر، هدف اصلی آزمایش‌ها سنجش میزان امنیت الگوریتم و مقاومت در برابر انواع حملات است. در آزمایش‌های انجام‌شده از الگوریتم ژنتیک دودویی با اندازه جمعیت ۱۰۰ استفاده‌شده است. برای هر متغیر ۱۶ بیت در

نظر گرفته‌شده است.

روش‌های استفاده‌شده در مراحل مختلف الگوریتم ژنتیک به شرح زیر می‌باشد: ۱- عملگر انتخاب: انتخاب تورنمنت[1]؛ ۲- مقیاس‌کردن شایستگی: انتخاب بولتزمن[2]؛ ۳- عملگر همبری: غیریکنواخت مبتنی بر ماسک الگو. ۴- تعداد تکرارها: ۳۰ تکرار. همچنین در تمام آزمایش‌ها نرخ جهش و همبری به ترتیب برابر با ۰/۰۵ و ۰/۹ است.

۴-۱- ۱-۴ تحلیل تفاضلی

تحلیل تفاضلی بر پایه میزان حساس‌بودن الگوریتم رمزنگاری در برابر تغییرات ورودی است. بدین معنا که کوچک‌ترین تغییر در ورودی حتی به‌اندازه یک بیت باید باعث تغییر حداقل ۵۰ درصدی در خروجی شود [۴۱]. این نوع تحلیل دارای دو معیار UACI و NPCR است [۴۲].

NPCR به‌عنوان درصد اختلاف تعداد پیکسل‌های دو تصویر رمز شده است که یکی از تصاویر؛ تصویر اصلی است و تصویر دوم، تصویر اصلی با یک تغییر جزئی خواهد بود. معیار NPCR طبق رابطه (۹) اندازه‌گیری می‌شود.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100$$
$$D(i,j) = \begin{cases} 0 & if\ E(i,j) = \acute{E}(i,j) \\ 1 & if\ E(i,j) \neq \acute{E}(i,j) \end{cases} \qquad (۹)$$

که W و H به ترتیب عرض و طول تصویر، $D(i,j)$ تفاوت بین پیکسل‌های متناظر تصویر رمزگذاری شده تصویر اصلی($E(i,j)$) و تصویر تغییریافته ($\acute{E}(i,j)$) را نشان می دهد.

UACI میانگین اختلاف بین دو تصویر (یک تصویر اصلی و یک تصویر تغییریافته) رمزنگاری شده را اندازه‌گیری می‌کند که طبق رابطه (۱۰) تعریف می‌شود.

$$UACI = \frac{\sum_{i,j} E(i,j) - \acute{E}(i,j)}{255 \times W \times H} \times 100 \qquad (۱۰)$$

در جدول (۱) نتایج آزمایش دو معیار UACI و NPCR برای تصویر رمز شده به ازای هر سه کانال رنگ آورده شده است. مقادیر UACI > ۳۳/۴٪ و NPCR > ۹۹/۶٪ تضمین می‌کند که یک الگوریتم رمزنگاری تصویر در برابر حمله تفاضلی مقاوم است [۴۳].

باتوجه‌به جدول (۱)، الگوریتم رمزنگاری دارای حساسیت مناسبی در برابر تغییرات جزئی است و توانسته است مقادیر بالایی برای دو معیار UACI و NPCR را کسب کند.

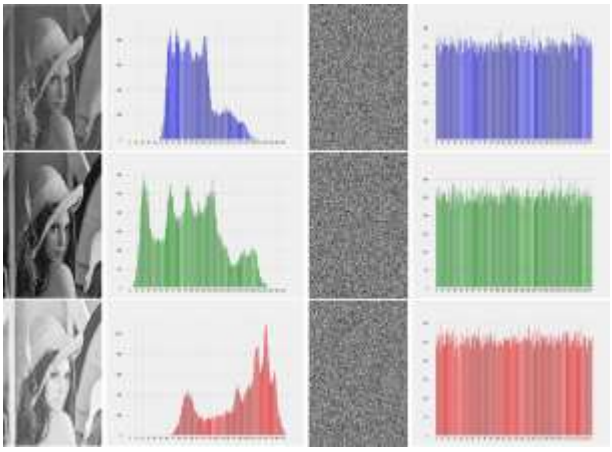
[1] Tournament selection
[2] Boltzmann selection

۴-۲- ۲-۴ تحلیل هیستوگرام

هیستوگرام[3] توزیع مقادیر پیکسل یک تصویر را نشان می‌دهد. هیستوگرام تصویر اصلی باید کاملاً با هیستوگرام تصویر رمزنگاری شده متفاوت باشد.

هیستوگرام تصاویر اصلی ماهیت غیریکنواختی دارند. درحالی‌که هیستوگرام تصاویر رمزنگاری شده باید ماهیت یکنواخت داشته باشند؛ یعنی همه پیکسل‌ها به طور مساوی در فضا توزیع‌شده باشند.

در شکل (۸) هیستوگرام تصویر، قبل و بعد از رمزنگاری ترسیم‌شده است. همان‌طور که گفته شد، هیستوگرام تصویر رمز شده به حالت یکنواخت تبدیل‌شده است.



شکل (۸). نمودار هیستوگرام تصویر نمونه لنا به ازای سه کانال رنگ، قبل و بعد از رمزنگاری

جدول (۱). مقادیر دو معیار NPCR و UACI برای شش تصویر نمونه

تصویر اندازه	معیار	کانال رنگ		
		قرمز	سبز	آبی
Lena 256	NPCR(%)	۹۹/۶۳۱۷	۹۹/۶۵۰۱	۹۹/۶۲۵۹
	UACI(%)	۳۳/۴۱۴۷	۳۳/۴۳۹۸	۳۳/۴۰۳۶
House 256	NPCR(%)	۹۹/۶۰۰۱	۹۹/۶۱۷۲	۹۹/۶۱۶۳
	UACI(%)	۳۳/۴۳۲۵	۳۳/۵۷۰۲	۳۳/۴۱۶۸
Jelly bean 256	NPCR(%)	۹۹/۶۱۶۹	۹۹/۶۲۲۱	۹۹/۶۱۵۶
	UACI(%)	۳۳/۴۱۱۸	۳۳/۴۱۹۸	۳۳/۴۲۶۰
Peppers 512	NPCR(%)	۹۹/۶۰۹۵	۹۹/۶۱۰۳	۹۹/۶۱۱۲
	UACI(%)	۳۳/۴۳۳۵	۳۳/۴۴۷۵	۳۳/۴۴۷۰

[3] Histogram

تصویر اندازه	معیار	کانال رنگ		
		قرمز	سبز	آبی
Mandrill 512	NPCR(%)	۹۹/۶۲۳۵	۹۹/۶۰۸۵	۹۹/۶۰۷۴
	UACI(%)	۳۳/۵۶۳۸	۳۳/۴۶۲۱	۳۳/۴۶۹۲
Aircraft 512	NPCR(%)	۹۹/۶۲۶۷	۹۹/۶۰۵۲	۹۹/۶۱۹۲
	UACI(%)	۳۳/۴۳۴۴	۳۳/۴۳۶۰	۳۳/۴۳۷۳
White 256	NPCR(%)	۹۹/۶۳۵۸	۹۹/۵۹۸۷	۹۹/۶۰۷۳
	UACI(%)	۳۳/۵۳۹۸	۳۳/۴۷۱۶	۳۳/۵۰۱۸
Black 256	NPCR(%)	۹۹/۶۱۵۰	۹۹/۵۸۹۷	۹۹/۶۰۸۱
	UACI(%)	۳۳/۴۲۵۸	۳۳/۳۹۸۳	۳۳/۴۱۹۷

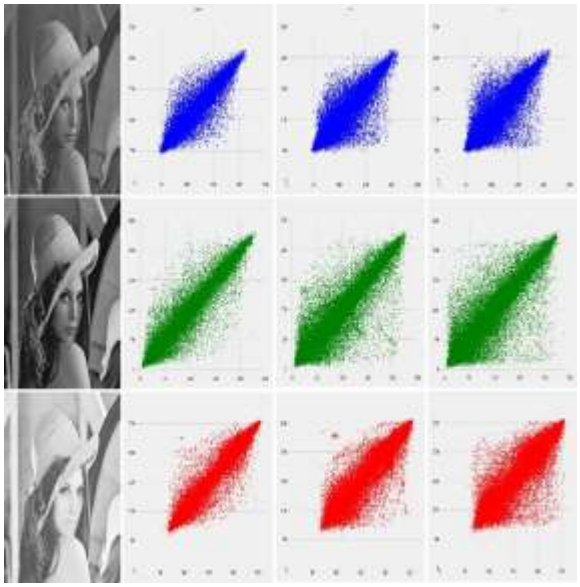
۴-۳- ۳-۴ ضریب همبستگی

ضریب همبستگی برای یافتن شباهت بین پیکسل‌های متناظر یک تصویر اصلی و رمزنگاری شده استفاده می‌شود. مقادیر پیکسل‌های مجاور یک تصویر اصلی در سه جهت افقی، مورب و عمودی دارای ضریب همبستگی بالایی هستند. درحالی‌که یک الگوریتم رمزنگاری مناسب ضریب همبستگی پیکسل‌های تصویر رمز شده را کاهش می‌دهد. ضریب همبستگی طبق رابطه (۱۱) محاسبه می‌شود.

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}}$$
$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K}$$
$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))^2 \qquad (۱۱)$$
$$D(y) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(y))^2$$

که $C(x,y)$ کوواریانس[1]، x و y مختصات تصویر، K تعداد جفت پیکسل‌های (x_i,y_i)، $D(x)$ و $D(y)$ به ترتیب انحراف معیار x و y، و $E(x)$ میانگین پیکسل های x_i است. در جدول (۲)، نتایج میزان همبستگی پیکسل‌های شش تصویر به ازای سه کانال رنگ، و برای هر سه جهت عمودی، افقی و قطری اندازه‌گیری شده است. باتوجه‌به مقادیر جدول (۲)، الگوریتم رمزنگاری به‌خوبی توانسته است همبستگی بین پیکسل‌ها را از بین ببرد.

همچنین برای درک بهتر چگونگی تغییر همبستگی پیکسل‌ها قبل و بعد از رمزنگاری، نمودار نقطه‌ای پیکسل‌ها به‌ازای سه کانال رنگ و سه جهت عمودی، افقی و قطری ترسیم‌شده است که در شکل‌های (۹) و (۱۰) نشان داده‌شده است.باتوجه‌به شکل (۹)، نمودارهای ترسیم‌شده همانند نمودار خطی تابع $f(x) = y$ است. بدین معنا که پیکسل‌ها دارای رابطه‌ای خطی هستند؛ اما در شکل (۱۰)، پس از رمزنگاری تصویر، روابط بین پیکسل‌ها به‌کلی از بین رفته است.



شکل (۹). نمودار نقطه‌ای همبستگی پیکسل‌های سه کانال رنگ برای تصویر لنا

[1] Covariance

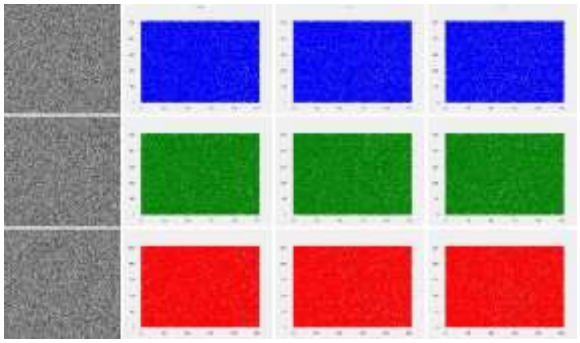
۴-۴- ۴-۴ آنتروپی

آنتروپی میانگین اطلاعات هر بیت در یک تصویر را اندازه‌گیری می‌کند که شامل اطلاعات احتمالی موجود در تصویر است. هر پیکسل مقدار متفاوتی دارد؛ بنابراین، آنتروپی یک تصویر رمزنگاری شده به این معنی است که هر پیکسل احتمال برابری با توزیع یکنواخت دارد. آنتروپی طبق رابطه (۱۲) محاسبه می‌شود.

$$H(S) = -\sum_{s} (P(s_i) \times log_2\ P(s_i)) \qquad (۱۲)$$

که $H(S)$ نشان‌دهنده محاسبه آنتروپی برای داده S، $P(s_i)$ احتمال رخداد s_i است. مقدار آنتروپی برای تصاویر ۸ بیتی بین بازه $[0,8]$ قرار می‌گیرد. برای بررسی میزان آنتروپی تصاویر رمزنگاری شده، آنتروپی شش تصویر نمونه پس از رمزنگاری محاسبه‌شده است و نتایج آن به ازای هر سه کانال رنگ در جدول (۳) آورده شده است.

باتوجه‌به جدول (۳) مقدار آنتروپی تمامی آزمایش‌ها بسیار نزدیک به حد نهایی آنتروپی (عدد ۸) برای یک تصویر ۸ بیتی است.



شکل (۱۰). نمودار نقطه‌ای همبستگی پیکسل‌های سه کانال رنگ برای تصویر رمز شده لنا

جدول (۳). مقدار آنتروپی شش تصویر نمونه پس از رمزنگاری به ازای سه کانال رنگ

تصویر اندازه	آنتروپی		
	قرمز	سبز	آبی
Lena 256	۷/۹۹۶۹	۷/۹۹۷۴	۷/۹۹۷۲
House 256	۷/۹۹۷۳	۷/۹۹۷۱	۷/۹۹۷۴
Jelly bean 256	۷/۹۹۷۲	۷/۹۹۷۱	۷/۹۹۷۰
Peppers 512	۷/۹۹۹۳	۷/۹۹۹۳	۷/۹۹۹۲
Mandrill 512	۷/۹۹۹۴	۷/۹۹۹۱	۷/۹۹۹۲
Aircraft 512	۷/۹۹۹۲	۷/۹۹۹۰	۷/۹۹۹۳
White 256	۷/۹۹۷۴	۷/۹۹۷۲	۷/۹۹۷۰
Black 256	۷/۹۹۷۱	۷/۹۹۷۳	۷/۹۹۶۸

۴-۵- ۴-۵ آزمایش داده‌های ازدست‌رفته

در این آزمایش فرض می‌شود که تصویر رمز شده در زمان انتقال

جدول (۲). مقادیر همبستگی پیکسل‌های کانال‌های رنگ تصاویر

تصویر اندازه	کانال رنگ	جهت همبستگی		
		افقی	عمودی	قطری
Lena 256	قرمز	-۰/۱۸۳۵	-۰/۱۵۴۶	-۰/۰۴۰۳
	سبز	-۰/۰۱۲۴	-۰/۱۸۱۷	-۰/۱۹۰۹
	آبی	-۰/۱۴۹۷	-۰/۰۹۵۹	-۰/۱۵۳۱
House 256	قرمز	-۰/۱۸۸۴	-۰/۱۰۶۰	-۰/۱۱۲۵
	سبز	-۰/۱۵۸۸	-۰/۱۰۰۱	-۰/۱۲۵۳
	آبی	-۰/۱۳۸۲	-۰/۰۹۷۶	-۰/۱۴۶۰
Jelly bean 256	قرمز	-۰/۰۸۲۴	-۰/۲۲۰۸	-۰/۱۹۱۰
	سبز	-۰/۲۶۹۵	-۰/۱۲۷۷	-۰/۰۹۷۳
	آبی	-۰/۰۳۳۴	-۰/۱۴۴۱	-۰/۲۴۴۸
Peppers 512	قرمز	-۰/۱۳۴۲	-۰/۱۹۶۷	-۰/۱۱۹۹
	سبز	-۰/۱۳۴۹	-۰/۱۶۴۷	-۰/۱۲۶۶
	آبی	-۰/۱۰۱۱	-۰/۱۶۷۰	-۰/۱۵۴۸
Mandrill 512	قرمز	-۰/۰۹۹۷	-۰/۱۵۳۲	-۰/۱۲۱۴
	سبز	-۰/۲۰۷۶	-۰/۰۹۸۵	-۰/۱۱۹۲
	آبی	-۰/۱۵۰۷	-۰/۰۸۷۳	-۰/۱۴۶۰
Aircraft 512	قرمز	-۰/۲۰۰۳	-۰/۱۰۳۹	-۰/۱۳۴۶
	سبز	-۰/۱۶۷۴	-۰/۲۵۴۵	-۰/۱۰۴۱
	آبی	-۰/۲۷۱۰	-۰/۱۲۶۹	-۰/۰۷۳۷
White 256	قرمز	-۰/۱۴۹۷	-۰/۱۰۵۸	-۰/۱۷۲۶
	سبز	-۰/۱۸۵۹	-۰/۱۵۳۰	-۰/۱۸۷۱
	آبی	-۰/۱۶۶۲	-۰/۰۹۸۰	-۰/۱۶۶۸
Black 256	قرمز	-۰/۱۵۷۳	-۰/۱۶۹۶	-۰/۱۴۲۰
	سبز	-۰/۱۳۸۹	-۰/۱۸۲۰	-۰/۱۲۳۵
	آبی	-۰/۱۳۶۲	-۰/۱۶۳۰	-۰/۰۹۹۷

به دست فردی مخرب می‌رسد و بخشی از تصویر را تخریب می‌کند که به نام حمله‌برش شناخته می‌شود. در این صورت زمان رمزگشایی تصویر، اطلاعات تصویر از بین رفته است و تصویر رمزگشایی‌شده، متفاوت از تصویر اصلی خواهد بود.

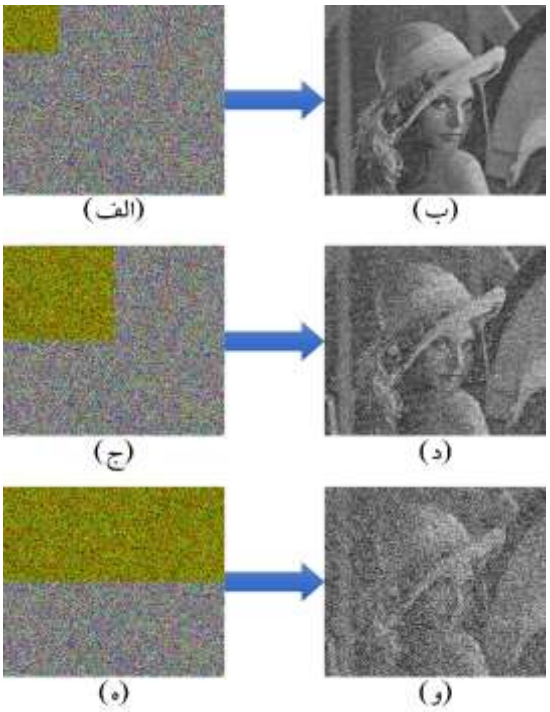
اگر الگوریتم رمزنگاری مناسب باشد (توزیع مناسب پیکسل‌ها، ازبین‌بردن اطلاعات آماری) حتی پس از تخریب بخشی از تصویر، تصویر رمزگشایی‌شده همچنان قابل‌استفاده خواهد بود و تنها بر اساس میزان تخریب، تصویر دچار نویز می‌شود.

به‌منظور سنجش مقاومت الگوریتم رمزنگاری در برابر حمله‌برش، تصویر رمزنگاری شده با درصدهای مختلفی تخریب می‌شود و سپس رمزگشایی می‌شود. نتایج آزمایش با درصد تخریب ۶٪، ۲۵٪ و ۵۰٪ برای کانال آبی تصویر نمونه لنا در تصویر (۱۱) قابل‌مشاهده است.

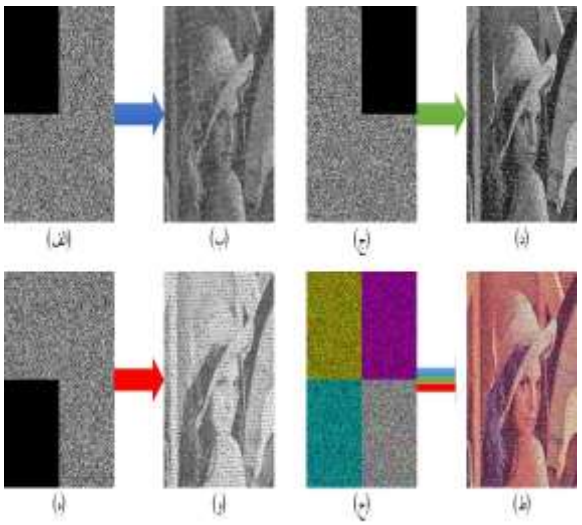
در آزمایش دیگری ۲۵ درصد هر سه کانال رنگ در موقعیت‌های متفاوت تخریب می‌شوند و تصویر رنگی نهایی رمزگشایی می‌شود. نتیجه آزمایش در شکل (۱۲) نشان داده‌شده است.

باتوجه‌به نتایج حاصل‌شده، می‌توان نتیجه گرفت که

الگوریتم رمزنگاری مقاومت مناسبی در برابر حمله‌برش دارد و حتی پس از تخریب بخشی از تصویر، تصویر رمزگشایی‌شده قابل‌استفاده است.



شکل (۱۱). مقاومت الگوریتم رمزنگاری در برابر حمله برش. (الف): تخریب ۶ درصد (ب): رمزگشایی تصویر «الف» (ج): تخریب ۲۵ درصد (د): رمزگشایی تصویر «ج» (ه): تخریب ۵۰ درصد (و): رمزگشایی تصویر «ه»



شکل (۱۲). مقاومت الگوریتم رمزنگاری در برابر حمله برش. (الف): تخریب ۲۵ درصد کانال آبی (ب): رمزگشایی تصویر «الف» (ج): تخریب ۲۵ درصد کانال سبز (د): رمزگشایی تصویر «ج» (ه): تخریب ۲۵ درصد کانال قرمز (و): رمزگشایی تصویر «ه» (ح): ترکیب کانال‌های رنگ رمز شده (ط): رمزگشایی تصویر «ح»

جدول (۴). کلیدهای رمز تغییریافته

کلید رمز	پارامترهای کلید
Key 1	$\{main\ \acute{v}ector,\ \sigma, \rho, \beta, a_b, b_b, a_g, b_g, a_r, b_r\}$
Key 2	$\{main\ vector,\ \acute{\sigma}, \rho, \beta, a_b, b_b, a_g, b_g, a_r, b_r\}$
Key 3	$\{main\ vector,\ \sigma, \acute{\rho}, \beta, a_b, b_b, a_g, b_g, a_r, b_r\}$
Key 4	$\{main\ vector,\ \sigma, \rho, \acute{\beta}, a_b, b_b, a_g, b_g, a_r, b_r\}$
Key 5	$\{main\ vector,\ \sigma, \rho, \beta, \acute{a_b}, b_b, a_g, b_g, a_r, b_r\}$
Key 6	$\{main\ vector,\ \sigma, \rho, \beta, a_b, \acute{b_b}, a_g, b_g, a_r, b_r\}$
Key 7	$\{main\ vector,\ \sigma, \rho, \beta, a_b, b_b, \acute{a_g}, b_g, a_r, b_r\}$
Key 8	$\{main\ vector,\ \sigma, \rho, \beta, a_b, b_b, a_g, \acute{b_g}, a_r, b_r\}$
Key 9	$\{main\ vector,\ \sigma, \rho, \beta, a_b, b_b, a_g, b_g, \acute{a_r}, b_r\}$
Key 10	$\{main\ vector,\ \sigma, \rho, \beta, a_b, b_b, a_g, b_g, a_r, \acute{b_r}\}$

جدول (۵). مقادیر NPCR برای تصویر رمز شده با کلید اصلی و تغییریافته.

کلید رمز	NPCR		
	قرمز	سبز	آبی
Key 1	۹۹/۶۰۴۶	۹۹/۵۸۷۰	۹۹/۵۹۳۰
Key 2	۹۹/۵۸۸۰	۹۹/۶۰۰۲	۹۹/۶۰۴۸
Key 3	۹۹/۶۰۴۲	۹۹/۶۱۶۴	۹۹/۵۸۵۱
Key 4	۹۹/۶۱۱۲	۹۹/۶۲۰۳	۹۹/۵۸۷۲
Key 5	۹۹/۶۰۴۰	۹۹/۵۸۶۷	۹۹/۵۸۱۶
Key 6	۹۹/۵۹۵۲	۹۹/۵۹۸۴	۹۹/۶۱۹۲
Key 7	۹۹/۵۸۵۵	۹۹/۵۸۲۸	۹۹/۶۲۹۱
Key 8	۹۹/۵۹۹۸	۹۹/۶۰۵۰	۹۹/۶۱۰۸
Key 9	۹۹/۶۰۸۵	۹۹/۶۲۶۲	۹۹/۶۱۴۸
Key 10	۹۹/۶۱۹۹	۹۹/۶۱۰۳	۹۹/۶۰۹۸

۴-۶- ۶-۴ تحلیل کلید رمز

همان‌طور که در بخش ۳-۷ اشاره شد، کلید رمزنگاری برای تصاویر رنگی و خاکستری، به ترتیب دارای ۸۰۰ و ۷۳۶ بیت است؛ بنابراین باتوجه‌به طول مناسب کلید، الگوریتم رمزنگاری در برابر حمله Brute Force مقاوم خواهد بود. از طرفی بخش ابتدایی کلید (۵۱۲ بیت ابتدا) چکیده سه داده کلید عمومی، بردار ویژگی‌های چهره و تصویر اصلی است؛ بنابراین تغییر یک بیت در داده‌های ذکرشده منجر به تغییر کل کلید رمز می‌شود، زیرا مقادیر اولیه نگاشت لورنز، از چکیده داده‌ها حاصل می‌شود. برای بررسی حساسیت الگوریتم رمزنگاری نسبت به کلید رمز، ابتدا تصویر نمونه را با کلید اصلی

$$Key = \{main\ vector, \sigma, \rho, \beta, a_b, b_b, a_g, b_g, a_r, b_r\}$$

رمزنگاری می‌شود. سپس هر بخش از کلید به طور مستقل دچار تغییری جزئی می‌شود و مابقی بخش‌های کلید ثابت می‌مانند. کلیدهای حاصل در جدول (۴) نشان داده‌شده‌اند.

تصویر لنا با هرکدام از کلیدها جداگانه رمزنگاری می‌شود. میزان NPCR هرکدام از تصاویر رمزنگاری شده با کلیدهای تغییریافته، با تصویر رمز شده توسط کلید اصلی محاسبه می‌شود. نتایج آزمایش در جدول (۵) نشان داده‌شده است.

باتوجه‌به مقادیر جدول (۵)، الگوریتم رمزنگاری حساسیت بالایی نسبت به تغییرات جزئی کلید دارد و با تغییر هر بخش از کلید رمز، تصویر رمز شده حاصل متفاوت خواهد بود.

۴-۷- ۴-۷ مقایسه نتایج الگوریتم پیشنهادی با سایر روش‌ها

در این بخش نتایج به‌دست‌آمده از روش پیشنهادی با سایر روش‌های ارائه‌شده درزمینهٔ رمزنگاری تصویر مقایسه می‌شود. نتایج مقایسه میزان همبستگی پیکسل‌های تصویر رمز شده، حملات تفاضلی و آنتروپی در جدول (۶) آورده شده است.

روش‌هایی که در جدول (۶) برای ارزیابی با روش پیشنهادی معرفی شده‌اند، در فاز جای‌گشت از روش‌هایی مانند مرتب سازی دنباله آشوب، عملگرهای همبری و جهش الگوریتم ژنتیک و مربع لاتین استفاده کرده‌اند. اما در روش پیشنهادی از الگوریتم فراابتکاری ژنتیک و نگاشت آشوب آرنولد جهت بهینه‌سازی همبستگی پیکسل‌ها استفاده شده است. باتوجه‌به جدول (۶)، روش پیشنهادی در مقایسه با سایر روش‌ها، بسیار موفق عمل کرده است و توانسته است همبستگی پیکسل‌ها را به‌صورت چشمگیری کاهش دهد؛ بنابراین روش پیشنهادی در مقابل حملات آماری مقاومت بالایی خواهد داشت. باتوجه‌به جدول (۶)، روش پیشنهادی در معیار همبستگی پیکسل‌ها در مقایسه با سایر روش‌ها، بسیار موفق عمل کرده است و توانسته است همبستگی پیکسل‌ها را در هر سه جهت افقی، عمودی و قطری به‌صورت چشمگیری کاهش دهد؛ بنابراین روش پیشنهادی در مقابل حملات آماری مقاومت بالایی خواهد داشت. همچنین روش‌هایی که برای ارزیابی با روش پیشنهادی انتخاب شده‌اند در فرآیند رمزنگاری از روش‌هایی مانند عملیات حسابی تنسورها، کدگذاری DNA، چکیده تصویر، دنباله‌های آشوب و عملگرهای الگوریتم ژنتیک استفاده کرده‌اند. باتوجه‌به اینکه در روش پیشنهادی از روش‌های چکیده تصویر، نگاشت‌های آشوب و الگوریتم فراابتکاری ژنتیک استفاده شده است، روش پیشنهادی توانسته است در آزمایش‌هایی موفق‌تر عمل کند و قابلیت رقابت با روش‌های مشابه را داشته باشد؛ بنابراین روش پیشنهادی در مقایسه با سایر روش‌های مشابه توانسته است نتایج مناسبی در آزمایش آنتروپی و تحلیل تفاضلی کسب کند.

۵- نتیجه‌گیری

در این مقاله یک روش جدید رمزنگاری تصویر مبتنی بر ویژگی‌های بیومتریک چهره و زنجیره‌بلوکی ارائه شده است که در فاز جانشینی از سه داده چکیده تصویر اصلی، بردار ویژگی‌های چهره و کلید عمومی برای تولید دنباله‌های شبه‌تصادفی استفاده شده است؛ بنابراین مقادیر دنباله‌ها بسیار وابسته به سه داده ذکرشده هستند و با تغییر یک بیت در هرکدام از داده‌ها، مقادیر دنباله‌های شبه‌تصادفی به‌کلی تغییر می‌کند. فاز جای‌گشت با استفاده از الگوریتم فراابتکاری ژنتیک کاراتر و بهینه‌تر انجام شد. در این فاز ابتدا یک جمعیت اولیه ساخته می‌شود که هرکدام از اعضای جمعیت دارای دو متغیر (دو متغیر نگاشت آرنولد) است.

تصویر توسط نگاشت آرنولد به‌ازای هرکدام از اعضای جمعیت جای‌گشت داده می‌شود و در هر مرحله جمعیت جدید بر اساس شایستگی ساخته می‌شود. پس از رسیدن به‌شرط توقف الگوریتم ژنتیک، بهترین عضو انتخاب، و تصویر جای‌گشت داده می‌شود. تابع شایستگی، مجموع وزن‌دار سه مقدار همبستگی پیکسل‌ها (افقی، عمودی و قطری) است. باتوجه‌به نتایج حاصل که در بخش ۴ بررسی شدند، الگوریتم رمزنگاری تأثیر چشمگیری در کاهش میزان همبستگی پیکسل‌ها و ازبین‌بردن اطلاعات آماری تصویر داشته است. همچنین نتایج آزمایش‌های مختلف انجام‌شده در بخش ۴، نشان می‌دهد که روش پیشنهادی در مقابل حملات آماری، حملات تفاضلی، حمله‌برش و حمله Brute Force مقاوم است.

پس از رمزنگاری تصویر، کلید رمزنگاری و بردار ویژگی‌های چهره توسط کلید عمومی رمزنگاری می‌شوند و به‌عنوان یک تراکنش در شبکه زنجیره‌بلوکی ذخیره می‌شوند. به‌منظور رمزگشایی تصویر یک فرآیند احراز هویت دومرحله‌ای انجام می‌پذیرد. در اولین مرحله با استفاده از کلید عمومی و خصوصی و در دومین مرحله به‌وسیلهٔ انطباق چهره کاربر، هویت فرد رمزنگار مشخص می‌شود که در صورت صحت هویت کاربر، کلید رمزنگاری در اختیارش قرار می‌گیرد.

در انتها باتوجه‌به ارزیابی‌ها و مقایسه‌هایی که برای روش پیشنهادی و سایر روش‌های مشابه که در بخش ۴-۷ انجام شد، می‌توان نتیجه گرفت که بخش‌های مختلف روش پیشنهادی مانند نگاشت‌های آشوب، الگوریتم ژنتیک، چکیده اطلاعات تصویر و چهره، کلید رمز، استراتژی رمزنگاری و احرازهویت به خوبی درکنار یکدیگر قرار گرفته‌اند و یک سیستم با عملکرد مناسب را شکل داده‌اند. باتوجه‌به جدول (۶)، روش پیشنهادی توانسته است یکی از اهداف اصلی الگوریتم رمزنگاری یعنی همبستگی پیکسل‌ها را به طور چشمگیری، نسبت به سایر روش‌های مقایسه شده کاهش دهد. همچنین الگوریتم پیشنهادی در معیارهای تفاضلی و آماری نیز توانسته است نتایج مناسبی را به دست آورد و در بسیاری از نتایج از روش‌های مشابه عملکرد بهتری داشته باشد.

جدول (۶). مقایسه نتایج روش پیشنهادی با سایر روش‌ها

تصویر کانال رنگ	معیار ارزیابی		الگوریتم					
			[۱۳]	[۱۴]	[۱۸]	[۲۴]	[۲۵]	روش پیشنهادی
لنا کانال قرمز	آنتروپی		۷/۹۹۷۲	۷/۹۹۱۷	۷/۹۹۹۴	۷/۹۹۷۳	۷/۹۹۷۲	۷/۹۹۶۹
	ضریب همبستگی	افقی	۰/۰۰۹۴	۰/۰۰۱۳	-۰/۰۰۰۲	۰/۰۰۴۶	۰/۰۰۸۳	-۰/۱۸۳۵
		عمودی	-/۰۰۱۱	۰/۰۰۴۷	-۰/۰۰۲۳	۰/۰۰۲۴	-۰/۰۰۵۴	-۰/۱۵۴۶
		قطری	۰/۰۰۰۹	۰/۰۰۰۲	-۰/۰۰۲۱	۰/۰۰۵۱	-۰/۰۰۱۰	-۰/۰۴۰۳
	تحلیل تفاضلی	NPCR	۹۹/۶۴۹۱	۹۹/۶۲۴۳	۹۹/۶۰۹۶	۹۹/۶۶۱۹	۹۹/۶۰۷۸	۹۹/۶۳۱۷
		UACI	۳۳/۳۸۲۷	۳۳/۴۲۲۴	۳۳/۴۵۹۹	۳۳/۶۱۷۷	۳۳/۵۶۴۴	۳۳/۴۱۴۷
لنا کانال سبز	آنتروپی		۷/۹۹۶۸	۷/۹۹۱۲	۷/۹۹۹۴	۷/۹۹۷۰	۷/۹۹۷۲	۷/۹۹۷۴
	ضریب همبستگی	افقی	-۰/۰۰۱۸	۰/۰۰۳۲	-۰/۰۰۰۲	-۰/۰۰۲۷	۰/۰۰۴۹	-۰/۰۱۲۴
		عمودی	-۰/۰۰۷۶	-۰/۰۰۰۵	-۰/۰۰۴۳	-۰/۰۰۰۷	۰/۰۱۰۰	-۰/۱۸۱۷
		قطری	۰/۰۰۰۶	۰/۰۰۴۸	۰/۰۰۰۷	-۰/۰۰۰۲	۰/۰۱۲۴	-۰/۱۹۰۹
	تحلیل تفاضلی	NPCR	۹۹/۶۱۶۳	۹۹/۶۱۸۵	۹۹/۶۱۰۷	۹۹/۶۲۷۲	۹۹/۶۶۷۸	۹۹/۶۵۰۱
		UACI	۳۳/۳۶۶۱	۳۳/۴۳۶۱	۳۳/۴۷۶۷	۳۳/۶۰۴۸	۳۳/۴۴۵۸	۳۳/۴۳۹۸
لنا کانال آبی	آنتروپی		۷/۹۹۷۶	۷/۹۹۱۷	۷/۹۹۹۴	۷/۹۹۷۲	۷/۹۹۷۵	۷/۹۹۷۲
	ضریب همبستگی	افقی	۰/۰۰۱۹	۰/۰۰۲۰	-۰/۰۰۷۴	-۰/۰۰۲۳	-۰/۰۰۱۷	-۰/۱۴۹۷
		عمودی	-۰/۰۰۴۲	۰/۰۰۰۱	-۰/۰۰۱۰	۰/۰۰۱۴	۰/۰۰۹۵	-۰/۰۹۵۹
		قطری	۰/۰۰۲۲	-۰/۰۰۴۰	-۰/۰۰۰۷	۰/۰۰۰۴	-۰/۰۰۴۲	-۰/۱۵۳۱
	تحلیل تفاضلی	NPCR	۹۹/۶۳۲۴	۹۹/۶۲۸۰	۹۹/۶۰۹۰	۹۹/۶۴۶۰	۹۹/۶۰۷۸	۹۹/۶۲۵۹
		UACI	۳۳/۴۵۷۷	۳۳/۴۶۰۳	۳۳/۴۳۳۳	۳۳/۶۴۲۲	۳۳/۵۰۵۵	۳۳/۴۰۳۶

۶- مراجع

[1]. M. Turculeț, "Ethical Issues Concerning Online Social Networks," *Procedia Soc Behav Sci*, vol. 149, pp. 967–972, 2014, doi: https://doi.org/10.1016/j.sbspro.2014.08.317.

[2]. S. Lian, *Multimedia content encryption: techniques and applications*. Auerbach Publications, 2008.

[3]. X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf Sci (N Y)*, vol. 486, pp. 340–358, Jun. 2019, doi: 10.1016/J.INS.2019.02.049.

[4]. H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 144, pp. 444–452, Mar. 2018, doi: 10.1016/J.SIGPRO.2017.11.005.

[5]. D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," *Signal Processing*, vol. 206, p. 108908, May 2023, doi: 10.1016/J.SIGPRO.2022.108908.

[6]. H. Ghadirli, A. Nodehi, R. E.-S. Processing, and undefined 2019, "An overview of encryption algorithms in color images," *Elsevier*, vol. 164, pp. 163–185, 2019, doi: 10.1016/j.sigpro.2019.06.010.

[7]. X. Wang and M. Zhao, "An image encryption algorithm based on hyperchaotic system and DNA coding," *Opt Laser Technol*, vol. 143, p. 107316, Nov. 2021, doi: 10.1016/J.OPTLASTEC.2021.107316.

[8]. S. Ma, Y. Zhang, Z. Yang, J. Hu, and X. Lei, "A New Plaintext-Related Image Encryption Scheme Based on Chaotic Sequence," *IEEE Access*, vol. 7, pp. 30344–30360, 2019, doi: 10.1109/ACCESS.2019.2901302.

[9]. X. J. Tong, M. Zhang, Z. Wang, Y. Liu, H. Xu, and J. Ma, "A fast encryption algorithm of color image based on four-dimensional chaotic system," *J Vis Commun Image Represent*, vol. 33, pp. 219–234, Nov. 2015, doi: 10.1016/J.JVCIR.2015.09.014.

[10]. N. Khalil, A. Sarhan, and M. A. M. Alshewimy, "An

color image encryption scheme based on 2DNLCML system and genetic operations," *Opt Lasers Eng*, vol. 128, p. 106040, May 2020, doi: 10.1016/J.OPTLASENG.2020.106040.

[25]. X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, "Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption," *Signal Processing*, vol. 183, p. 108041, Jun. 2021, doi: 10.1016/J.SIGPRO.2021.108041.

[26]. L. S. Khan, M. M. Hazzazi, M. Khan, and S. S. Jamal, "A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes," *Chinese Journal of Physics*, vol. 72, pp. 558–574, Aug. 2021, doi: 10.1016/J.CJPH.2021.03.029.

[27]. Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain," *Opt Laser Technol*, vol. 135, p. 106610, Mar. 2021, doi: 10.1016/J.OPTLASTEC.2020.106610.

[28]. R. Li, "Fingerprint-related chaotic image encryption scheme based on blockchain framework," *Multimed Tools Appl*, vol. 80, no. 20, pp. 30583–30603, Aug. 2021, doi: 10.1007/S11042-020-08802-Z/METRICS.

[29]. G. Boeing, "Visual Analysis of Nonlinear Dynamical Systems: Chaos, Fractals, Self-Similarity and the Limits of Prediction," *Systems 2016, Vol. 4, Page 37*, vol. 4, no. 4, p. 37, Nov. 2016, doi: 10.3390/SYSTEMS4040037.

[30]. N. A. Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map," *Egyptian Informatics Journal*, vol. 17, no. 1, pp. 139–146, Mar. 2016, doi: 10.1016/J.EIJ.2015.10.001.

[31]. G. Qu *et al.*, "Optical color image encryption based on Hadamard single-pixel imaging and Arnold transformation," *Opt Lasers Eng*, vol. 137, p. 106392, Feb. 2021, doi: 10.1016/J.OPTLASENG.2020.106392.

[32]. E. N. Lorenz, "Deterministic Nonperiodic Flow," *J Atmos Sci*, vol. 20, no. 2, pp. 130–141, Mar. 1963, doi: 10.1175/1520-0469(1963)020.

[33]. S. Katoch, S. S. Chauhan, and V. Kumar, "A review on genetic algorithm: past, present, and future," *Multimed Tools Appl*, vol. 80, no. 5, pp. 8091–8126, Feb. 2021, doi: 10.1007/S11042-020-10139-6/FIGURES/8.

[34]. A. Bodo, "Method for producing a digital signature with aid of a biometric feature," *German patent DE*, vol. 42, no. 43, p. 908, 1994.

[35]. V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, Dec. 2019, doi: 10.1007/S41939-019-00049-Y/METRICS.

[36]. C. Bisogni, G. Iovane, R. E. Landi, and M. Nappi, "ECB2: A novel encryption scheme using face biometrics for signing blockchain transactions," *Journal of Information Security and Applications*, vol. 59, p. 102814, Jun. 2021, doi: 10.1016/J.JISA.2021.102814.

[37]. N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," *Proceedings - 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR 2005*, vol. I, pp. 886–893, 2005, doi: 10.1109/CVPR.2005.177.

[38]. O. Déniz, G. Bueno, J. Salido, and F. De La Torre, "Face recognition using Histograms of Oriented Gradients," *Pattern Recognit Lett*, vol. 32, no. 12, pp. 1598–1603, Sep. 2011, doi: 10.1016/J.PATREC.2011.01.004.

[39]. K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint Face efficient color/grayscale image encryption scheme based on hybrid chaotic maps," *Opt Laser Technol*, vol. 143, p. 107326, Nov. 2021, doi: 10.1016/J.OPTLASTEC.2021.107326.

[11]. T. Wang and M. hui Wang, "Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding," *Opt Laser Technol*, vol. 132, p. 106355, Dec. 2020, doi: 10.1016/J.OPTLASTEC.2020.106355.

[12]. S. Zhou, "A real-time one-time pad DNA-chaos image encryption algorithm based on multiple keys," *Opt Laser Technol*, vol. 143, p. 107359, Nov. 2021, doi: 10.1016/J.OPTLASTEC.2021.107359.

[13]. J. Zhou, N.-R. Zhou, and L.-H. Gong, "Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix," *Opt Laser Technol*, vol. 131, p. 106437, Nov. 2020, doi: 10.1016/J.OPTLASTEC.2020.106437.

[14]. D. Zhang, L. Chen, and T. Li, "Hyper-Chaotic Color Image Encryption Based on Transformed Zigzag Diffusion and RNA Operation," *Entropy 2021, Vol. 23, Page 361*, vol. 23, no. 3, p. 361, Mar. 2021, doi: 10.3390/E23030361.

[15]. H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Processing*, vol. 113, pp. 104–112, Aug. 2015, doi: 10.1016/J.SIGPRO.2015.01.016.

[16]. X. Chai, X.-L. Chai, Z.-H. Gan, Y. Lu, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *iopscience.iop.org*, vol. 25, no. 10, p. 100503, 2016, doi: 10.1088/1674-1056/25/10/100503.

[17]. E. Zarei Zefreh, "An Image Encryption Algorithm Based on the Sn Permutation Group and Chaotic Functions" *Journal of Electronical & Cyber Defence*, vol. 8, no. 3, pp.139–150,2020,dor: 20.1001.1.23224347.1399.8.3.11.5 (In Persian)

[18]. Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimed Tools Appl*, vol. 80, no. 9, pp. 13841–13864, Apr. 2021, doi: 10.1007/S11042-020-10437-Z/METRICS.

[19]. S. Zhou, X. Wang, Y. Zhang, B. Ge, M. Wang, and S. Gao, "A novel image encryption cryptosystem based on true random numbers and chaotic systems," *Multimed Syst*, vol. 28, no. 1, pp. 95–112, Feb. 2022, doi: 10.1007/S00530-021-00803-8.

[20]. R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata," *Opt Lasers Eng*, vol. 71, pp. 33–41, Aug. 2015, doi: 10.1016/J.OPTLASENG.2015.03.007.

[21]. R. Enayatifar, A. H. Abdullah, and M. Lee, "A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption," *Opt Lasers Eng*, vol. 51, no. 9, pp. 1066–1077, Sep. 2013, doi: 10.1016/J.OPTLASENG.2013.03.010.

[22]. S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, "Optimizing chaos based image encryption," *Multimed Tools Appl*, vol. 77, no. 19, pp. 25569–25590, Oct. 2018, doi: 10.1007/S11042-018-5807-X.

[23]. A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *AEU - International Journal of Electronics and Communications*, vol. 66, no. 10, pp. 806–816, Oct. 2012, doi: 10.1016/J.AEUE.2012.01.015.

[24]. Y. Q. Zhang, Y. He, P. Li, and X. Y. Wang, "A new

Detection and Alignment Using Multitask Cascaded Convolutional Networks," *IEEE Signal Process Lett*, vol. 23, no. 10, pp. 1499–1503, Oct. 2016, doi: 10.1109/LSP.2016.2603342.

[40]. F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 07-12-June-2015, pp. 815–823, Oct. 2015, doi: 10.1109/CVPR.2015.7298682.

[41]. H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Processing*, vol. 164, pp. 163–185, Nov. 2019, doi: 10.1016/J.SIGPRO.2019.06.010.

[42]. M. Kaur and V. Kumar, "A Comprehensive Review on Image Encryption Techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, Jan. 2020, doi: 10.1007/S11831-018-9298-8/METRICS.

[43]. M. Essaid, I. Akharraz, A. Saaidi, and A. Mouhib, "A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map," *Procedia Comput Sci*, vol. 127, pp. 539–548, Jan. 2018, doi: 10.1016/J.PROCS.2018.01.153.