Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

A secure and robust stereo image encryption algorithm based on DCT and Schur decomposition

S. Kumar*

*Corresponding author, Assistant Prof., Department of Mathematics, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, 248007, India. E-mail: sanoj.kumar@ddn.upes.ac.in

M. K. Singh

Assistant Professor, Department of Mathematics, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, 248007, India. E-mail: mkumar@ddn.upes.ac.in

G. Dobhal

Assistant Professor, Department of Mathematics, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, 248007, India. E-mail: gdobhal@ddn.upes.ac.in

D. Saini

Assistant Professor, Department of Mathematics, Graphic Era Deemed to be University, Dehradun, Uttarakhand, 248002, India. E-mail: deepikasaini@geu.ac.in

G. Bhatnagar

Associate Professor, Department of Mathematics, Indian Institute of Technology Jodhpur, Rajasthan, 342037, India. E-mail: goravb@iitj.ac.in

Abstract

Security solutions of stereo images are always a major concern during the transmission and communication. In this manuscript, a simple yet efficient framework for encrypting stereo images is formulated using discrete cosine transform (DCT), generalized logistic map, Schur decomposition and magic square method. The framework initiated with the integration of DCT and generalized logistic map to unify both pair of images. This unified image is then encrypted using the Schur decomposition and magic square method. The various experiments and analysis have been done to explore the validity, proficiency and performance of the purport framework.

Keywords: Stereo Image; Encryption and Decryption; Discrete Cosine Transform; Generalize Logistic Map; Schur Decomposition.

DOI: https://10.22059/jitm.2022.85647 Manuscript Type: Research Paper University of Tehran, Faculty of Management

Received January 07, 2021 Accepted March 25, 2021

Introduction

In this era due to the development of internet technology, multimedia transmission has gained importance and hence its security is a major concern for all. Multimedia security includes copyright protection, authentication and access control. As wireless networks has made easy to build, transmit, retroflex and dispense digital substance protection and therefore implementation of cerebral controls for digital world has become a crucial consequences (Menezes A. J., et al 1997). Cryptography using encryption and decryption techniques ensures security during the multimedia communication. Cryptography is the technique of disguising a message so that authorized recipient can understand it. Image can be encrypted using various algorithms, most effective in terms of computational cost is DES (Stinson D. R., et al 2018). Image can encrypt cipher image using symmetric or asymmetric keys (Chang C.C., et al 2001). In asymmetric ciphers, public and private keys are used (Huijuan X., et al 2007). The methodology used in encryption and decryption algorithm is important, like key streams in OTP, prime in RSA, secrete key in DES algorithm and invariant DC coefficients (Ali M., et al 2020) so on. Conventionally, image encryption is performed through techniques such as RGB color shuffling, chaotic mapping method and bit manipulations. Thus, the image gets converted into cipher image, most of the method lead to cryptosystem with slow transmission speed.

Digital media can be transmitted to the frequency orbit by various method: DCT (Alturki F. T., et al 2007), DFT (Knockaert L., et al 1999), FrFT (Lin C., et al 2001), DWT (Agreste S., et al 2008), SVD (Mohammad A., et al 2008). In order to improve the result of different methods, various approaches are combined e.g. SVD-DWT (Bhat K. V., et al 2011), SVD-DCT (Singh S., et al 2018) and DWT-DFT (Amirgholipour S.K., et al 2009). Here, the Schur decomposition has been used which is rich against various attacks including JPEG compression geometrical distortion (Kumar S., et al 2019). The scrambling of multimedia elements results in mystification by the change of their position and hence original multimedia is not discernible. The original multimedia can be reverted back using reverse operations. In order to intensify the security, the image undergoes for scrambled into another phase by using various reversible techniques such as magic squares transform, gray code, chaos system, Arnold transform, fractal Hilbert curve and others (Liu X., et al 2004). Sometimes, the image is also passed through various algorithms like

SCAN (Maniccam S.S., et al 2004). This method is able to produce the different types of space filling curves. In this framework, the image is first decomposed into vectors for sequential encoding. Different types of algorithms were purposed for the same e.g. a mirror like image encryption (Guo J.I., et al 2020), zigzag transformation scrambling (Dong H., et al 2011), an optical encryption system using grey scale (Qin Y., et al 2016), grey-level visual cryptography (Yamaguchi Y., 2014), zigzag permutation technique (Droogenbroeck M., et al 2002), shuffle encryption algorithm (SEA) (Yahya A., et al 2008), block based transformation algorithms (Chuang T., et al 1999), also known as Blowfish encryption and decryption technique and security of stereo images (Kumar S., et al 2012).

Recently, Secret Image Sharing (SIS) was the main focus of the researchers. For sharing purpose, a confidential image is partitioned into many shadows. Since, these shadows are easily available for attacks. So, to overcome from this problem, a secure and effective algorithm based on DWT based SIS with authentication (DWT-SISA) is proposed (Xiong L., et al 2020). In this work, the researchers have discussed many issues such as the meaningless generated shadows which are easy for attacks, dishonorable companion would sprit shadows to lampoon and outflow of secret image. Some other techniques are also available which used Galois field (Haq T. U., et al 2020). The image ciphered framework based on spatiotemporal chaotic system is described (Wang X., et al 2020). An image is transformed into SHA-512 to produce the axiom keys. These keys are furnished into LDCML spatiotemporal chaos field. A modified SVD-based blind color image watermarking approach with assorted modulation is investigated (Hu H. T., et al 2020, Singh M. K., et al 2020). The process of watermark embedding assist to protect the orthogonality in the unitary matrix and indemnify for the consequential deformation. While the latest version of this technique did not perform well enough against JPEG compression, speckle noise and Gaussian noise.

This manuscript report a novel secure and robust stereo image ciphered framework. The proposed framework is based on the magic square scrambling method, discrete cosine transform, generalized logistic map and Schur decomposition. In the first phase, scrambling of pixels positions is completed by magic square scrambling method followed by discrete cosine transform. The pixel values are modified in the next phase by using generalized logistic map and Schur decomposition. The singular values of a random matrix which are generated by Schur decomposition is used to generate the two random matrices (one for left and another for right stereo images, respectively) as the secret keys. With the help of these secret keys, a secret information is gathered by both (left and right) singular vectors. The ciphered mechanism for both the stereo images is performed with the help of these secret matrices (keys). At the last, both the encrypted pair of images are unified into a single image. This image is now treated as the final ciphered image and then it is transmitted through an insecure network channel. At the recipient end, final ciphered image is extracted into left and right ciphered stereo images. The decryption process starts after the extraction procedure. The performance and the robustness of the described framework are illustrated by various experiments. The efficiency of the algorithm is also explained with statistical, numerical and noise analysis.

Mathematical Preliminaries

Discrete Cosine Transform (DCT)

In DCT, the data is represented in terms of frequency and hence it makes watermarking technique more robust in comparison to spatial domain techniques. DCT separates parts of images into different frequencies. In the quantization process during compression, frequencies having less importance are discarded. The remaining frequencies are used to retrieve the image in decompression mechanism. The distortion, thus produced can be adjusted during the compression process. If (r,s) represent the spatial coordinates and (p,q) represent the coordinates in DCT domain, then $2D$ discrete cosine transform of a signal is defined as

$$F(p,q)=\frac{2}{\sqrt{mn}}C(p)C(q)\sum_{r=0}^{m-1}\sum_{s=0}^{n-1}f(r,s)\times\cos\left(\frac{(2r+1)p\pi}{2m}\right)\cos\left(\frac{(2s+1)q\pi}{2n}\right)$$

$$\text{where } C(p),C(q)=\begin{cases}\frac{1}{\sqrt{2}} & p,q=0\\ 1 & p,q\neq 0\end{cases} \qquad (1)$$

where $m\,,n$ represents the size of a signal. Similarly, $2D$ inverse discrete cosine transformation is defined as

$$f(r,s)=\frac{2}{\sqrt{mn}}C(p)C(q)\sum_{p=0}^{m-1}\sum_{q=0}^{n-1}F(p,q)\times\cos\left(\frac{(2r+1)p\pi}{2m}\right)\cos\left(\frac{(2s+1)q\pi}{2n}\right)$$

$$\text{with } F(0,0)=\frac{1}{\sqrt{mn}}\sum_{r=0}^{m-1}\sum_{s=0}^{n-1}f(r,s) \qquad (2)$$

Generalized Logistic Map

Chaos theory deals with nonlinear mathematics, physics and philosophy. It deals with nonlinear mathematical phenomenon and therefore unpredictable like weather, turbulence, stock market and so on. Chaos shows highly deterministic behavior and is susceptible to its initial behavior. The future behavior of the scheme is highly sensible to its initial values. The dynamical system depends upon the mathematical formulation which predict the behavior of the system and is called a chaotic map. One dimensional chaotic system has high efficiency level and simplicity, but with a small key space. With increase in control parameter and initial condition chaotic system become highly complex having big key space. Mathematically chaotic mapping is defined in space onto itself.

$$h:T\to \mathrm{T},\ \ \mathrm{T}\subset \mathrm{R} \tag{3}$$

where T is defined mostly in the closed interval $[0,1]$ or $[-1,1]$. The mapping can be defined as

$$k_{x+1}=h(k_x,t), \tag{4}$$

where y_0 denotes the initial value of the system. With g as non-linear, a sequence is obtained as

$$k_1=h(k_0,t), \tag{5}$$

$$k_2=h(k_1,t)\Rightarrow k_2=h(f(k_1,t),t), \tag{6}$$

$$k_3=h(k_2,t)\Rightarrow k_3=h(h(h(k_1,t),t),t), \tag{7}$$

and so on. The sequence $k_1,k_2,k_3,....$ is known as trajectory or orbit generated by y_0. In a dynamic system, we study the characteristics of the orbits for periodicity and analyze the nature as $x\to\infty$. Logistic map is a case of chaotic maps describing the growth in population with respect to time and is given as

$$k_{x+1}=tk_x(1-k_x) \tag{8}$$

where $x=1,2,3,...n$, $0\le t\le 4$. The map is in the indiscriminate stage for $3.5699\le t\le 4$. The non-uniform character and blank ports in the indiscriminate areas are removed in generalized logistic map (Bhatnagar G., et al 2012) and defined as

$$k_{x+1}[1+4(t^2-1)k_x(1-k_x)]=4tk_x(1-k_x) \tag{9}$$

where $x=1,2,3,...n$, $-1.7\le t\le -0.3598$. The map is in the chaotic state for $-0.8795\le t\le -0.4324$The effectiveness and chaoticity is measured by Lyapunov exponent (LE), if it is positive for all values of t then the system is chaotic.

Schur Decomposition

If $A\in \mathrm{R}^{n\times n}$ is a matrix of the gray-scale image, then an orthogonal matrix $Q\in \mathrm{R}^{n\times n}$ exits such that

$$Q^T AQ=\begin{bmatrix} A_{11} & A_{11} & ... & A_{1m} \\ .. & A_{22} & ... & A_{2m} \\ .. & .. & ... & A_{mm} \\ & & & \end{bmatrix}=R=D+N \tag{10}$$

is an upper quasi-triangular matrix. Q is an unitary matrix and each block A_{ii} are a square matrix of order 1×1 or 2×2. Every 1×1 block equates to a real eigenvalue of A and 2×2 block equates to the couple of complex conjugate eigenvalues of A. The column of Q are known as Schur vectors. D is a diagonal matrix consisting of eigenvalues of A and N is strictly upper triangular matrix. The column partition q_i of the matrix Q are known as Schur vectors and we have $Aq_k = \lambda_k q_k + \sum_{i=1}^{k-1} N_{ik} q_i$. Therefore the subspaces $S_k = span(q_1, q_2, ..., q_k)$ are invariant. If a matrix $A \in \mathrm{C}^{n\times n}$ is normal, then a unitary matrix $Q \in \mathrm{C}^{n\times n}$ exist in a way that $Q^T AQ = diag(\lambda_1, ...)$ which confirms that Schur and the eigenvalue decompositions of a normal matrix are same. In case of a symmetric positive definite matrix, the Schur decomposition co-occur with SVD. Schur decomposition shows stability and its vector are unaffected by scaling.

Proposed Algorithm

In this segment, the incite ingredients to design the proposed stereo image coding algorithm via ciphered technique are mentioned. This algorithm starts with a stereo image pairs and these pairs are united into a single ciphered image. At the decoder end, the ciphered images are spilt into two parts succeed by the decryption process for various purposes. $F_I : I \in \{L, R\}$ describes the original stereo images. The size of both image pairs is $M \times N$. The puport framework can be described as:

Encryption Process

1. Take left and right stereo image pairs.

2. Scrambling both the rectangular stereo image pairs by magic square scrambling method (Lin K. T., et al 2011) and obtain $\left(I_L^S \text{and } I_R^S\right)$.

3. Apply discrete cosine transform (DCT) on both scrambling stereo image pairs and obtain $\left(I_L^{S,dct} \text{and } I_R^{S,dct}\right)$.

4. Adopting keys k_1, k_2 and k_3 as the primitive source, iterate generalized logistic map to produce three random sequences K_1, K_2 and K_3 of length $M\times M$, $N\times N$ and $M\times N$, respectively.

5. Transform all the received chaotic sequences K_i in previous step into integer sequences $\hat{K}_i$ as follows

$$\hat{K}_i = \left(255\times\frac{K_i+1}{2}\right) \tag{11}$$

where $i = 1, 2, 3$.

6. Arrange random integer sequences into arrays of size $M \times M$, $N \times N$ and $M \times N$ respectively. Let these arrays are denoted by K_i , $i = 1,2,3$.

7. Apply schur decomposition on the arrays K_i , $i = 1,2$.

$$\mathrm{K}_i = U_i * T_i * U_i^T . \tag{12}$$

8. Obtain the matrix keys as follows $Key_1 = U_1$ and $Key_2 = U_2$.

9. Both the stereo images are encrypted in DCT domain as

$$I_L^e = Key_1 * I_L^{S,dct} * Key_2^T$$

$$I_R^e = Key_1 * I_R^{S,dct} * Key_2^T \tag{13}$$

10. Finally, both ciphered images are combined into an individual image which is described as final ciphered image and obtained as follows

$$I_{final}^e(:,:,i) = \begin{cases} I_L^e, & if \;\; i = 1 \\ \mathrm{K}_3, & if \;\; i = 2 \\ I_R^e, & if \;\; i = 3 \end{cases} \tag{14}$$

Decryption Process

1. Both the ciphered images are teared from the final ciphered image (I_{final}^e). This process is borrowed by the equation.

$$\begin{cases} I_{L1}^e = I_{final}^e(:,:,1) \\ I_{R1}^e = I_{final}^e(:,:,3) \end{cases} \tag{15}$$

2. By adopting keys $\{k_i : i = 1,2\}$, **steps 2** to **7** of ciphered procedure are executed to obtain the matrix keys K_i .

3. The matrix keys help to receive the decrypted images from I_{L1}^e and I_{R1}^e i.e.

$$I_\ell^d = inv(\mathrm{K}_i) I_\ell^e \Rightarrow \begin{cases} I_{L1}^d = \mathrm{K}_1^T I_{L1}^e \\ I_{R1}^d = \mathrm{K}_2^T I_{R1}^e \end{cases} \tag{16}$$

The received matrix keys (K_i) are the orthogonal matrices, therefore, $inv(\mathrm{K}_i) = \mathrm{K}_i^T$.

4. Apply the inverse DCT on both the image pairs I_{L1}^{d} and I_{R1}^{d}, to obtain the decrypted scrambling left and right stereo image pairs, denoted by $I_{L}^{d,S}$ and $I_{R}^{d,S}$, respectively.

5. Finally, perform the descrambling by inverse magic square scrambling method to obtain final decrypted left and right stereo image pairs, denoted by I_{L}^{d} and I_{R}^{d}, respectively.

Results

MATLAB platform is exploited to examine the performance, robustness and efficiency of the purport stereo image coding framework. Many experiments are performed on different stereo image pairs namely Teddy, Aloe Vera, Baby and Laundry. The size of each stereo image pair is 450×375. The stereo images which are used in this study are shown in Figure 1. The visual outcomes are shown for Teddy stereo image only whereas other outcomes are shown for all the stereo image pairs. First of all, both the stereo images are scrambled by the magic square matrix method (Lin K. T., 2011) and the results for the same are shown in the Figure 2. Mainly three parameters are used as the keys $key_i : i = 1, 2, 3$ in the proposed algorithm. These keys are taken as the starting guess for the iterative generalized logistic map. Out of three keys, first two keys are adopted to generate keys in the form of matrix. $key_1 = 0.0056$ and $key_2 = 0.8756$ are set as initial guess for both images, respectively. The third key, $key_3 = 0.5689$, has no such importance as compared to first two keys with respect to the security of the proposed framework.

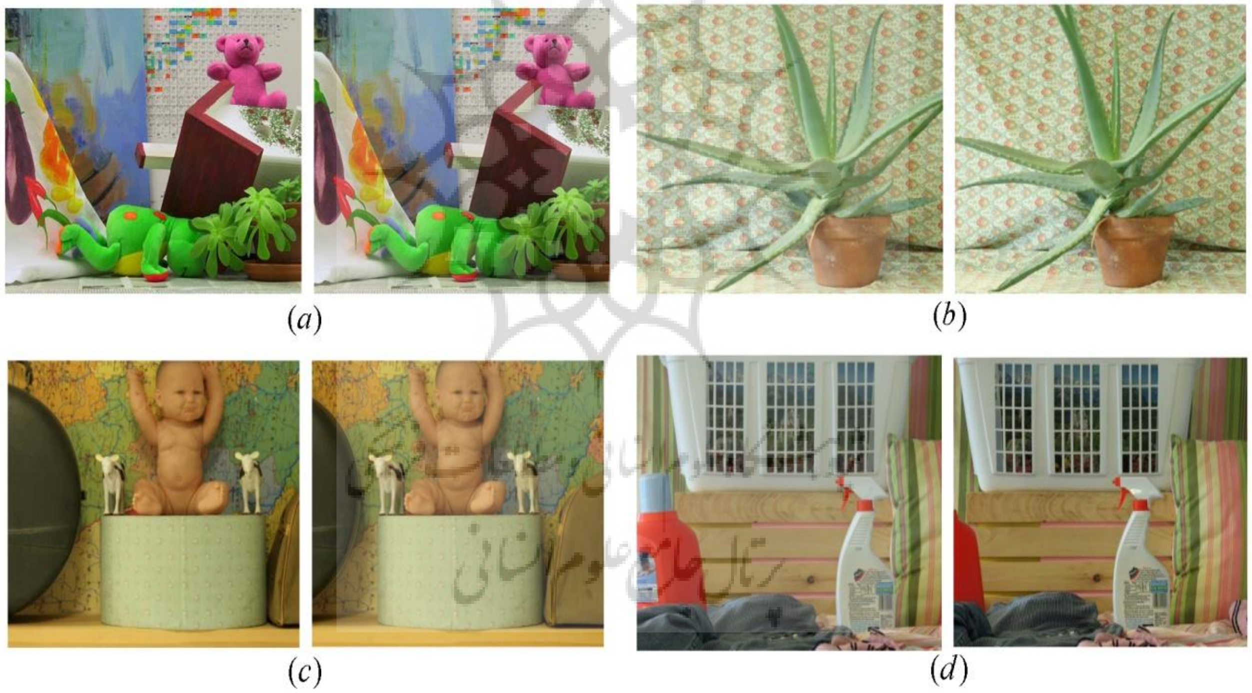

Figure 1. Stereo image pairs (*a*) Teddy, (*b*) Aloe Vera, (*c*) Baby and (*d*) Laundry.

It is adopted only to combined both the stereo image pairs into an single image. Thus, two keys (*key*$_1$ and *key*$_2$) encounter a critical part in the surity of the purport algorithm. The ciphered and deciphered Teddy stereo image pairs are mentioned in Figure 3 (*a–i*). Security is always a big concern of the encryption algorithms. There should not be so much deviation in encryption algorithms against the attacks of the type like brute-force, statistical and cryptanalytic. The detailed analysis of these metrics are explained as:

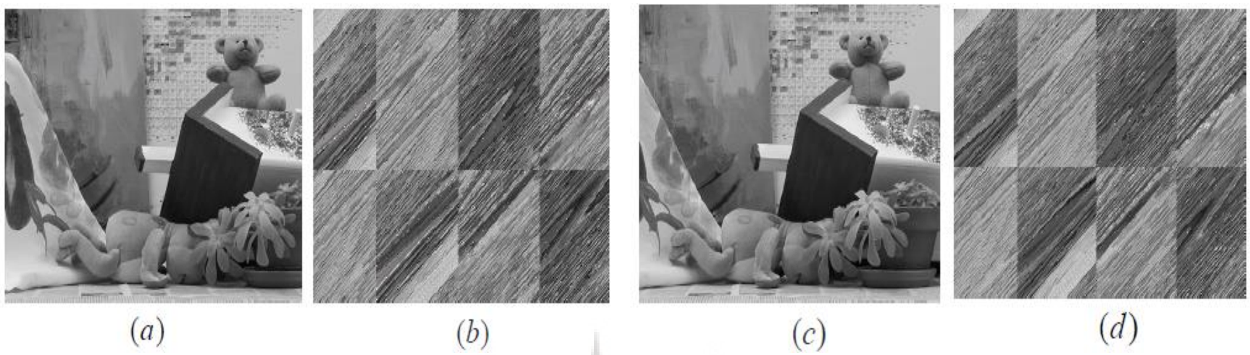

Figure 2. Scrambling process: (*a*) Teddy left stereo image, (*b*) Scrambling Teddy left stereo image, (c) Teddy right stereo image, and (d) Scrambling Teddy right stereo image.

Key Sensitivity Analysis

The encryption and decryption algorithms are very sensitive against keys. The principle says that a minor change in keys which are used to encrypt the data never produces the complete decryption for a remarkable security. To examine this effect on the proposed algorithm, two keys $\left(key_i : i = 1, 2\right)$ are adopted. key_1 and key_2 are used to encrypt both stereo image pairs, respectively. The ciphered image is mentioned in the Figure 3 (*a*). The deciphered images are adverted in the Figures 3 (*b-i*). Figure 3 (*b-c*) exhibit the decrypted stereo images when both the keys are correct, Figure 3 (*d-e*) shows the decrypted left and right stereo images when the key_1 is wrong and key_2 is correct, Figure 3 (*f,g*) represents the deciphered stereo images when the key_1 is correct and key_2 is wrong and Figure 3 (*h-i*) represents the deciphered stereo images when both the keys are wrong, respectively. Here, the values of the keys are changed in such a way that that older values (*key*$_1$=0.0056, *key*$_2$=0.8756) and newer values $\left(key_1 = 0.0056466, key_2 = 0.875611\right)$ are very close to each other. From the results, one can observed that if the deciphered stereo images are considered with updated keys then according to the human visual system, there is always a dissimilarity between the original and the deciphered stereo images. Therefore, a modest modification in any one the keys results a imperfect decryption. This analysis confirm that the purport algorithm is so sensitive against keys.

Visual Similarity Analysis

The hidden information which a sender wants to transmit over an insecure channel is important, so an encryption algorithm assures that this information must not be outflow to the assaulters. The statistical analysis is another mode to analyze the performance of any encryption framework.

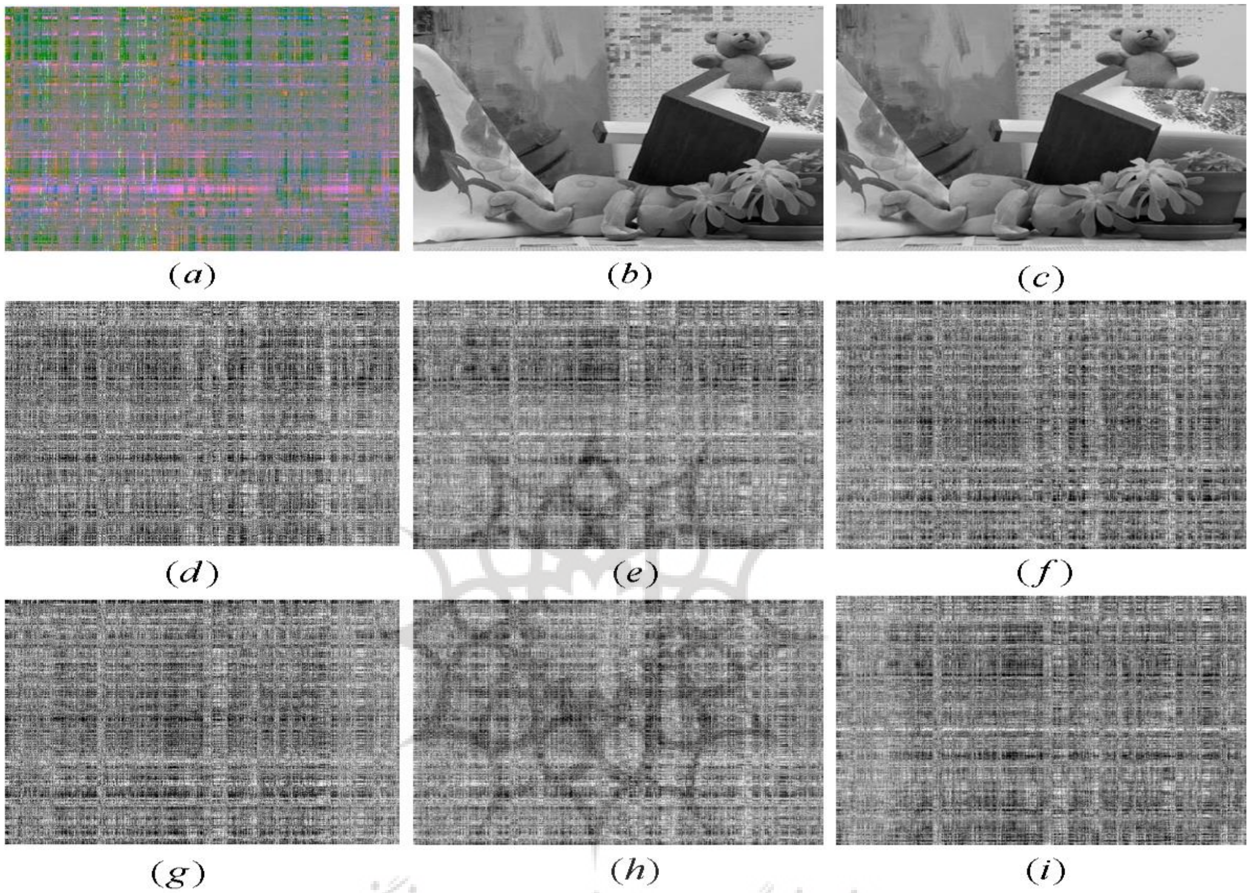

Figure 3. Ciphered results: (*a*) Final ciphered image; decrypted stereo image pairs with: (*b,c*) all exact keys, (*d,e*) inexact key_1, (*f,g*) inexact key_2, (*h,i*) all inexact keys.

Histogram and correlation analysis are the two metrics which are elected to measure the functioning of the proposed algorithm. According to histogram analysis, a consistent variation in the histogram of an image after encryption decide that the purport framework performs well. No one can measure the dispersion of the original signal if there is a uniform histogram of that signal or image. In this case, the valuable information is not pass to the assaulters. Figures 4(*a,b*) mentioned the histogram of the original left and right stereo image pairs. Figures 4 (*c,d*) mentioned the histograms of the ciphered stereo image pairs. From these figures, it is elucidated that the histogram is uniformly spreaded. Hence, the proposed ciphered framework works well and does not give any hint to the attackers about the original stereo images.

Correlation analysis is selected to analyze the kinship between two signals. If the correlation is high then it suggests a strong relationship between the images while if the value of the correlation is low then it means that the images have a weak relationship between them. For a good encryption algorithm this kinship among the neighboring points of a data or image must be break. If the value of the correlation is far away from 1 then it shows that the algorithm is good. For this analysis, we

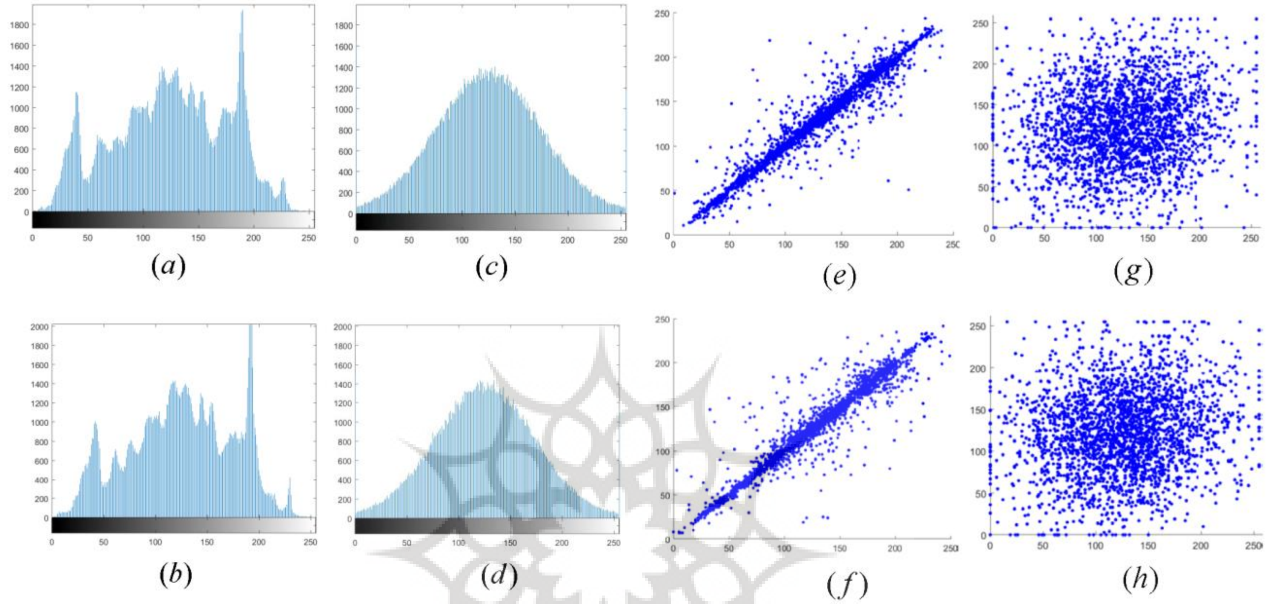

Figure 4. Histogram results: (*a,b*) histogram of original stereo image pairs; (*c,d*) ciphered stereo image pairs; Correlation results: correlation diagram of two neighboring pixels in horizontal direction in (*e,f*) original stereo images (*g,h*) ciphered stereo images.

selected randomly 3000 adjacent pixels in the direction of horizontal, vertical and diagonal. Now, the correlation is evaluated between two neighboring pixels in all the directions. The mathematically formula to calculate the correlation between two neighboring pixels is defined as

$$C_{r,s} = \frac{E[(r-E(r))(s-E(s))]}{\sqrt{E(r^2)-(E(s))^2}\sqrt{E(s^2)-(E(s))^2}} \tag{17}$$

where r and s are the gray values of two neighboring picture elements and $E()$ refers the expected (mean) value. Here, the visual results of the correlation coefficients have shown in the Figure 4 for the neighboring pixels in horizontal direction of the original and encrypted stereo images. The correlation dispersion of two neighboring pixels in the original and ciphered stereo images are mentioned in the Figures 4(*e,f*) and 4(*g,h*), respectively. The statistical results of correlation coefficients in all three pointllism are cited in Table 1. It is spectacular from the Figure 4 as well as from the Table 4 that the pixels of ciphered left and right stereo images are not correlated. Hence, the purport framework breaks the rich correlation between the neighboring pixels in stereo images.

Peak Signal to Noise Ratio (PSNR)

PSNR is a very significant aspect to measure the conformity between the data or images. It is computed in many areas of image processing to check the similarity e.g. image compression, watermarking, image coding and biometrics. If the bit depth of the images is 8 bits then generally the value of PSNR lies in the range $0-50$. The higher measure of PSNR indicates the better conformity of the data or images. If two images are identical then value of PSNR between them is infinite. If x_{rs} and y_{rs} are the corresponding pixels at rs^{th} position of the first and second images, respectively then mathematically, PSNR is defined as

Table1. Normalized correlation coefficients of two neighboring pixels in original and ciphered images.

Normalized Correlation Coefficient in	**Images**		**Direction**		
			Horizontal	**Vertical**	**Diagonal**
Original Stereo Images	**Teddy**	Left	0.9654	0.9570	0.9382
		Right	0.9630	0.9509	0.9324
	Aloe Vera	Left	0.9667	0.9426	0.9249
		Right	0.9648	0.9392	0.9203
	Baby	Left	0.9838	0.9847	0.9728
		Right	0.9824	0.9829	0.9701
	Laundry	Left	0.9350	0.9662	0.9087
		Right	0.9302	0.9655	0.9029
Encrypted Stereo Images	**Teddy**	Left	0.1170	0.1160	0.0840
		Right	0.1380	0.0450	0.0940
	Aloe Vera	Left	0.0330	0.0330	0.0260
		Right	0.0430	0.0450	0.0320
	Baby	Left	0.0780	0.0890	0.0660
		Right	0.0760	0.0800	0.0630
	Laundry	Left	0.0960	0.0760	0.0580
		Right	0.0860	0.0690	0.0460

$$PSNR = 10\log_{10}\frac{255^2}{\frac{1}{RS}\sum_{r=1}^{R}\sum_{s=1}^{S}[x_{rs}-y_{rs}]^2} \tag{18}$$

where RS is the total number of picture elements in a image. The results for PSNR on the different stereo images (Teddy, Aloe Vera, Baby and Laundry) are shown in the Table 2. The high value of PSNR suggests a good uniformity between the decrypted and encrypted stereo images.

Universal Image Quality Index (UIQI)

The UIQI is measured to investigate the structural similarity betwixt the original data and the distorted data. It breaks the comparison between two images in terms of contrast and luminance. The UIQI falls in the interval $[-1,1]$ and if UIQI is near to 1 then it shows a rich similarity between the data. Mathematically, UIQI is given as

$$UIQI = \frac{\sigma_{xy}}{\sigma_x \sigma_y} \cdot \frac{2\mu_x \mu_y}{\mu_x^2 + \mu_y^2} \cdot \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2} \tag{19}$$

where μ_x, μ_y, σ_x, σ_y and σ_{xy} have their usual meanings. The outcomes are mentioned in the Table 2. SSIM is an improved interpretation of the UIQI.

Structural similarity index measure (SSIM)

It is another way to determine the conformity between two signals. The value of SSIM always lies in the interval $[-1,1]$. It shows the greater conformity between the signals when its value is near to 1. SSIM is given be the equation

$$SSIM = \frac{[2\mu_x \mu_y + D_1][2\sigma_{xy} + D_2]}{[\mu_x^2 + \mu_y^2 + D_1][\sigma_x^2 + \sigma_y^2 + D_2]} \tag{20}$$

where D_1, D_2 are two variables which are used to brace the partition with a minor value in the denominator. When the value of SSIM is 1 then the images are identical. From the Table 2, the values of SSIM for different stereo images suggest a good similarity between the images.

Spectral Distortion (SD)

The spectral distortion can be defined as a measure of unsuitable match between images based on their spectral attributes. The similarity between images according to their spectral information is measured by spectral distortion. The higher value of SD shows a bad similarity in the images while the lower value of SD indicates a good similarity in the images. If x_{rs} and y_{rs} are the corresponding pixels at rs^{th} position of the first and second images, respectively then spectral.

Table 2. PSNR, UIQI, SSIM, and SD analysis for the proposed algorithm.

Stereo Images		PSNR	UIQI	SSIM	SD
Teddy	Left	37.3777	0.00002	0.00009	59.4385
	Right	37.1937	0.00200	0.00110	57.9559
Aloe Vera	Left	35.0107	0.00040	0.00023	45.0891
	Right	34.8236	0.00210	0.00130	44.1016

Baby	Left	37.3777	0.00017	0.00010	53.3582
	Right	35.9602	0.00090	0.00090	50.6731
Laundry	Left	35.7705	0.00110	0.00080	49.2582
	Right	35.3292	0.00020	0.00022	46.7137

distortion is defined as

$$SD = \frac{1}{RS}\sum_{r=1}^{R}\sum_{s=1}^{S}| x_{rs} - y_{rs} | \qquad (21)$$

where $R \times S$ is the size of an image. The outcomes of SD are mentioned in Table 2.

Information Entropy Analysis

The information entropy first was proposed by Shannon (Shannon C. E., 1948) in his theory of communication. The entropy is determined exclusively by the probability distribution of the source. It is a criterion of the precariousness in information theory associated with a random variable. Generally, the entropy measures the information carried out in the image (data) in the form of bits (Wang X., et al 2015). It tells the length of minimum message which is necessary to pass the information. Now, we take an example to explain this fact. A long string in which the characters are repeated has entropy is 0. The reason for this is that every character is predictable.

Mathematically, the entropy, represented by $H(Z)$, is defined as

$$H(Z) = \sum_{z=0}^{L-1} P(Z_z) log_2 \frac{1}{P(Z_z)} \qquad (22)$$

where $P(Z_z)$ denotes the probability of the outcomes Z_z of a random variable Z and the random

Table 3. Information Entropy Analysis

Stereo Images		Information Entropy
Teddy	Left Image	7.6311
	Right Image	7.6102
Aloe Vera	Left Image	7.2577
	Right Image	7.2526
Baby	Left Image	7.5150
	Right Image	7.4664
Laundry	Left Image	7.4457
	Right Image	7.3960

variable has L values. Let us assume that a source produces $L = 2^8$ values with equal probability. By using the above equation, one can estimate the entropy $H(Z) = 8$. If the entropy of a ciphered data is very near to 8 then the encryption process make a random like encrypted data. In this study, entropy for all the encrypted stereo images are estimated and results are exhibited in Table 1. With the help of Table 1, one can noticed that the estimated entropy is very near to 8. Therefore, it is prominent that the escape of the information in the encrypted stereo images is negligible.

Noise Analysis

The execution of the purport algorithm is also examined with different types of noises e.g. Gaussian, salt & paper and speckle noise. First, any one of these noises is added to both the original stereo image pairs. Second, the whole process of the proposed algorithm is applied on these noisy stereo images. An encrypted image always suffers with some kind of noises which are already present in the insecure channel. Therefore, the proposed algorithm must be so strong that the effect of the noises should be minimum. In this section, we have discussed this fact clearly. The detailed descriptions of the results under various noises are explained as below.

Gaussian Noise

It follows the probability distribution function namely Gaussian distribution (Li J., 2016). The noise takes the values which are Gaussian distributed. White Gaussian noise, a special case of Gaussian noise, is in which the amounts of it at any brace of times are uniformly spread. Statistically, it is independent. Due to these two facts, the white Gaussian noise are uncorrelated in nature. The Gaussian noise is added with mean 0 and variance are 0.01, 0.10 and 0.50. The visual results in all three cases are mentioned in the Figure 5. Figures 5(a, d, g) exhibit noisy left teddy image; Figures 5(b, e, h) exhibit the decrypted left teddy image, and Figures 5(c,f,i) exhibit the final encrypted image with Gaussian noise of mean 0 and variance 0.01, 0.10 and 0.50, respectively.

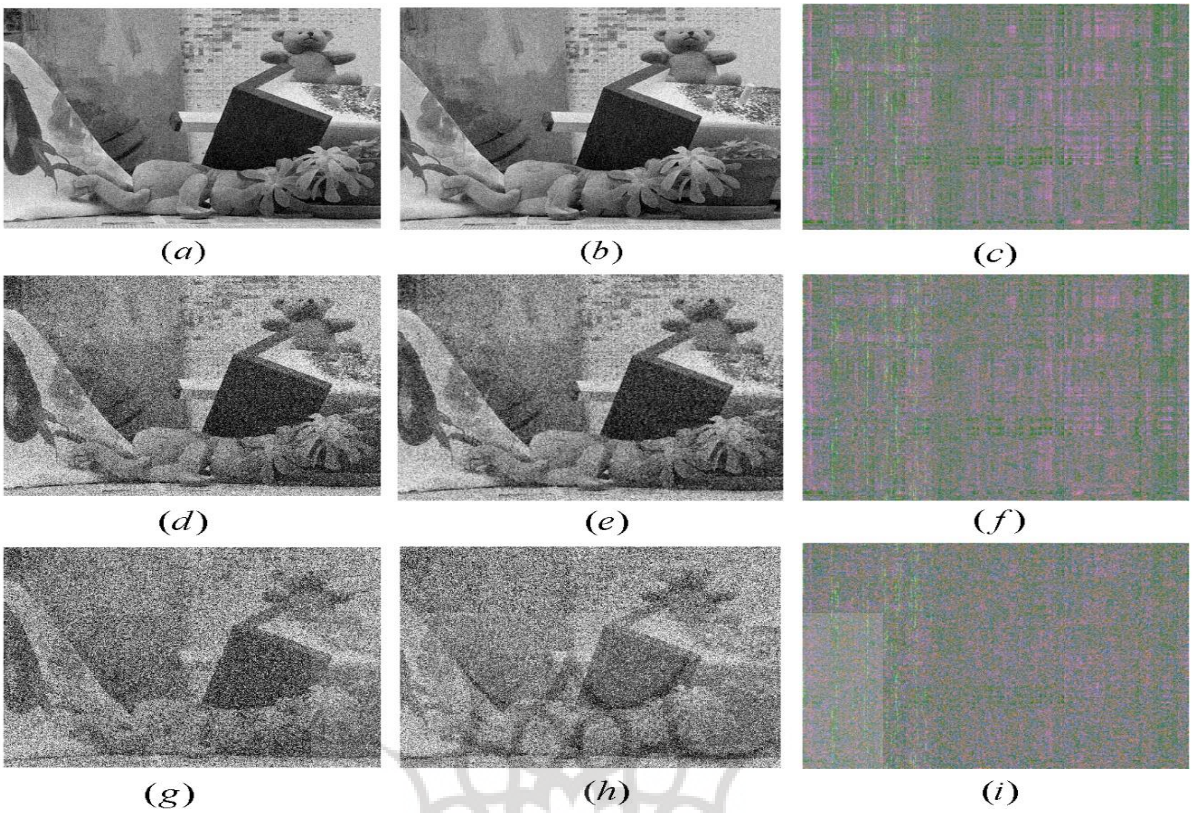

Figure 5. Gaussian noise results:(*a, d, g*) noisy left teddy images, (*b, e, h*) noisy decrypted left teddy images, (*c, f, i*) final encrypted images with Gaussian noise of mean 0 and variance 1%, 10% and 50%, respectively.

Salt & Pepper Noise

This noise arises in many signals (images) when there are sudden and sharp changes in those signals (images) (Jithin K., et al 2020). Based on this fact an image having salt & pepper noise can be characterized into two categories: (1) dark areas with bright pixels and (2) bright areas and dark pixels. To reduce the effects of such noises, median filter, morphological filter and algorithms based on dark frame subtractions are used. Sometimes the interpolation also used around the dark or bright pixels to shorten the effects of it. In our analysis, we added the salt & pepper noises to the original stereo images with 5%, 10% and 50% density. The results in the case of salt & pepper noise are mentioned in Figure 6. Figures 6 (*a*, *d*, *g*) exhibit noisy left teddy images, Figures 6 (*a*, *d*, *g*) exhibit decrypted left teddy image and Figures 6 (*a*, *d*, *g*) exhibit the final encrypted image with 5%, 10% and 50% density of salt and pepper noise.

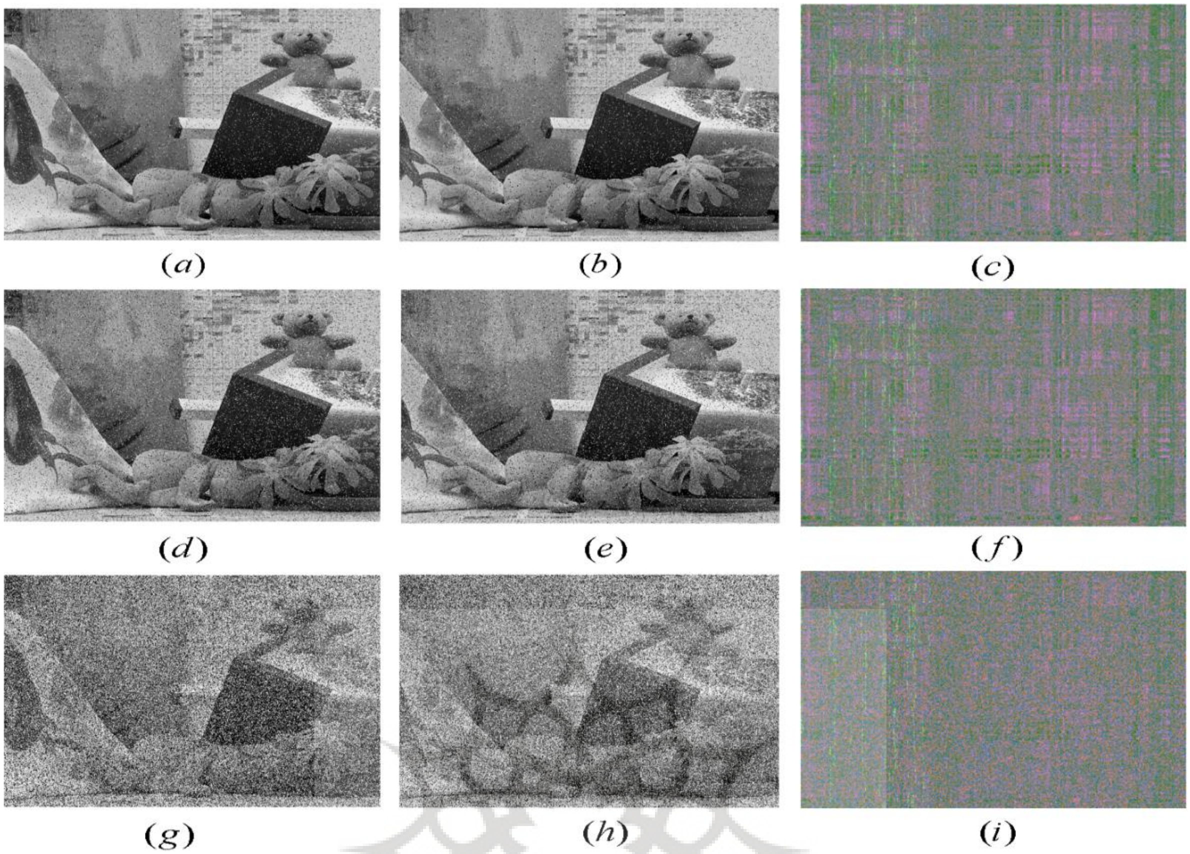

Figure 6. Salt & pepper noise results: (*a, d, g*) noisy left teddy images, (*b, e, h*) noisy decrypted left teddy image, and (*c, f, i*) final encrypted images with 5%, 10% and 50% density, respectively.

Speckle Noise

Sometimes the environmental conditions of imaging sensors are effected so badly during image acquisition. Because of this, the noise which already presents in the images is known as the speckle noise. Mostly, the speckle noise arises in medical images, SAR images and active Radar images (Li J., et al 2018). Various filtering techniques are used to overcome such kind of noises. In our analysis, we added the speckle noise with variance 0.05, 0.10 and 0.50 to the original stereo images. The results in the case of speckle noise are mentioned in the Figure 7. Figures 7(a, d, g) exhibit noisy left teddy images, Figures 7 (b, e, h) exhibit decrypted left teddy image and Figures 7(a, d, g) represent the final encrypted image with variance 0.05, 0.10 and 0.50, respectively.

Conclusions

In this work, a secure and robust stereo image encryption algorithm for stereo images based on generalized logistic map, DCT and Schur decomposition is explained. Magic square matrix method is used to scramble the stereo image pairs whereas DCT, generalized logistic map and Schur decomposition are used to generate the secret key matrices. Both the stereo image pairs are unified to make a single image with the help of these secret key matrices. This image further transmitted through an insecure channel. The efficiency, performance and robustness are validated with several experiments. The security analysis of the algorithm demonstrated that descent combination of the secret matrices is significant and much required to expose the stereo image pairs. The statistical analysis suggested the randomness of the algorithm for encrypted stereo images. The noise analysis proved that the proposed algorithm performs quite well when there are disturbance in the images. Overall analysis admits the suitability and attainability of our techniques to secure the stereo image pairs during communication and transmission. In future work, our aim to incorporate the machine learning tools to the encryption algorithm which will further boost up it and apply these algorithms for medical images also.

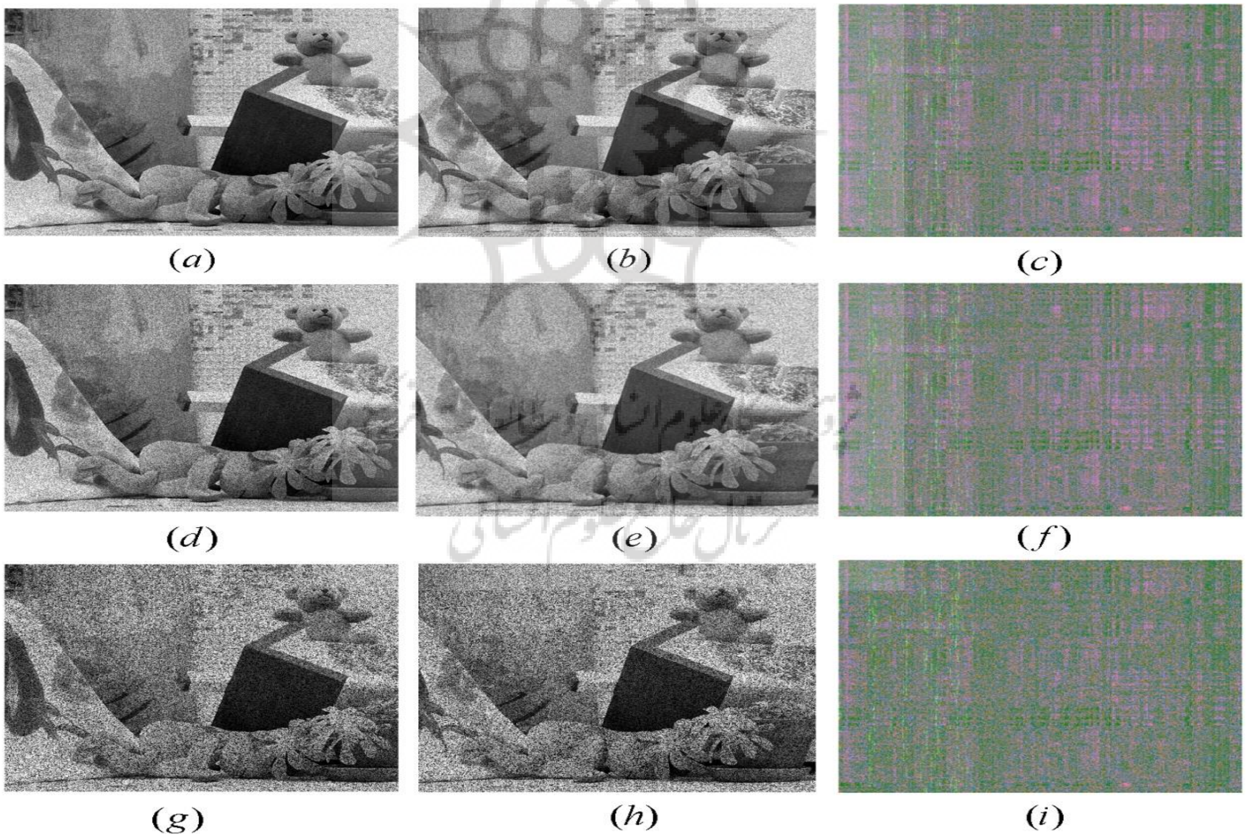

Figure 7. Speckle noise results: (*a, d, g*) noisy left teddy images: (*b, e, h*) noisy decrypted left teddy image, (*c, f, i*) final encrypted images with speckle noise with variance 0.05, 0.10 and 0.50, respectively.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article

References

Agreste S. & Andaloro G. (2008). A new approach to pre-processing digital image for wavelet-based transform. *Journal of Computational and Applied Mathematics*, 221(2), 274-283.

algorithm with mixed modulation incorporated. *Information Sciences*, 519, 161-182.

Ali M., Ahn C. W., Pant M., Kumar S., Singh M. K., Saini D. (2020). An optimized digital watermarking scheme based on invariant DC coefficients in spatial domain. *Electronics*, 9 (9), 14-28.

Alturki F. T., Almutairi A., & Mersereauu R, M. (2007). Analysis of blind data hiding using discrete cosine transform phase modulation. *Signal Processing and Image Communication*, 22(4), 347–362.

Amirgholipour S.K. & Naghsh-Nilchi A. R. (2009). Robust digital image watermarking based on joint DWT-DCT. *IEEE Transaction on Image Processing*, 3(2), 42–54.

based on spatiotemporal chaotic system. *Optik*, 217, 64884,

based secret image sharing with authentication. *Signal Processing*, 173, 107571.

Bhat K. V., Sengupta I., & Das A. (2011). A new audio watermarking scheme based on singular value decomposition and quantization. *Circuit, System and Signal Processing*, 30(5), 915–927.

Bhatnagar G. & Wu Q. M. J. (2012). Selective image encryption based on pixels of interest and singular value decomposition. *Digital Signal Processing*, 22, 648-663.

Chang C. C., Hwang M. S., & Chen T. S. (2001). A new encryption algorithm for image cryptosystems. *The Journal of System and Software*, 58, 83-91.

Chuang T. & Lin J. (1999). A new multiresolution approach to still image encryption. *Pattern Recognition and Image Analysis*, 9(3), 431–436.

compressed images. *In: Advanced Concepts for Intelligent Vision Systems*, (pp. 90–97).

Dong H., Lu P., & Ma X. (2011). Image scrambling algorithm based on mixed chaotic systems and extended zigzag transformation. *Computer Engineering and Design*, 32(4), 1241–1245.

Droogenbroeck M. & Benedett R. (2002). Techniques for a selective encryption of uncompressed and

Guo J.I. & Yen J. C. (2000). A new mirror-like image encryption algorithm and its VLSI architecture. *Pattern Recognition and Image Analysis*, 10(2), 236–247.

Haq T.U. & Shah T. (2020). 12×12 S-box Design and its Application to RGB Image Encryption. *Optik*,

Hu H.T., Hsu L. Y., & Chou H. H. (2020). An improved SVD-based blind color image watermarking

Huijuan X., Shuisheng Q., Chengliang D. , Zhong H. Y., & Ying C. (2007, November). A composite image encryption scheme using aes and chaotic series. *In: The First International Symposium on Data, Privacy, and E-Commerce* (*ISDPE*), (pp. 277–279).

Images. *In Transactions on Data Hiding and Multimedia Security IX*, (pp. 25–41).

Knockaert L., Backer B., & Zutter D. (1999). SVD compression, unitary transforms, and computational complexity. *IEEE Transaction on Signal Processing*, 47(10), 2724-2729.

Kumar S., Bhatnagar G. (2019). SIE: an application to secure stereo images using encryption. *In Handbook of Multimedia Information Security: Techniques and Applications*, (pp. 37-61).

Kumar S., Bhatnagar G., Raman B., Sukavanam N. (2012). Security of stereo images during communication and transmission. *Advanced Science Letters*, 6 (1), 173-179.

Lin C., Wu M., Bloom M. J., Cox I. J., Miller M., & Lui Y. (2001). Rotation, scale, and translation resilient watermarking for images. *IEEE Transaction on Signal Processing*, 10(5), 767-782.

Lin K.T. (2011). Hybrid encoding method by assembling the magic-matrix scrambling method and the binary encoding method in image hiding. *Optics Communication*, 284, 1778–1784.

Liu X. (2004). Four alternative patterns of the Hilbert curve. *Applied Mathematics and Computation*, 147(3), 675-685.

Maniccam S.S. & Bourbakis N.G. (2004). Image and video encryption using SCAN patterns. *Pattern Recognition*, 37(4), 725–737.

Menezes A. J., Oorschot P. C. V., & Vanstone S. (1997). *In Handbook of Applied cryptography*, Vol. 1. CRC Press.

Mohammad A., Alhaj A., & Shaltaf S. (2008). An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Processing*, 88(9), 2158–2180.

Qin Y., Wang H., Wang Z., Gong Q., & Wang D. (2016). Encryption of QR code and grayscale image in interference-based scheme with high quality retrieval and silhouette problem removal. *Optics and Lasers in Engineering*, 84, 62-73.

Shannon C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, 27(3), 379–423.

Singh M. K., Kumar S., Ali M., Saini D. (2020). Application of a novel image moment computation in X-ray and MRI image watermarking. *IET Image Processing*, 15(3), 666-682.

Singh S. P. & Bhatnagar G. (2018). A new robust watermarking system in integer DCT domain. *Journal of Visual Communication and Image Representation,* 53, 86-101.

Stinson D. R. & Paterson M. (2018). *In Cryptography: Theory and Practice*, Vol. 1. CRC Press.

Wang X. & Yang J. (2020). A novel image encryption scheme of dynamic S-boxes and random blocks

Xiong L., Zhong X., & Yang C. N. (2020). DWT-SISA: a secure and effective discrete wavelet transform

Yahya A. & Abdalla A. (2008). A shuffle image encryption algorithm. *Journal of Computer Science*,

Yamaguchi Y. (2014). Extended Visual Cryptography Scheme for Multiple-Secrets Continuous-Tone

Wang X., Liu L., & Zhang Y. (2015). A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Optics and Lasers in Engineering*, 66, 10–18.

Li J. (2016). Asymmetric multiple-image encryption based on octomom Fresnel transform and sine logistic modulation map. *Journal of the Optical Society of Korea*, 20(3), 341–357.

Jithin K. & Sankar S. (2020). Colour image encryption algorithm combining, Arnold map, DNA sequence operation, and a Mandelbrot set. *Journal of Information Security and Applications*, 50(102428).

Li J., Xiang S., Wang H., Gong J., & Wen A. (2018). A novel image encryption algorithm based on synchronized random bit generated in cascade-coupled chaotic semiconductor ring lasers. *Optics and Lasers in Engineering*, 102, 170-180.

Bibliographic information of this paper for citing:

Kumar, S. ; Singh, M. K. ; Dobhal, G.; Saini, D. & Bhatnagar, G. (2022). A secure and robust stereo image encryption algorithm based on DCT and Schur decomposition. *Journal of Information Technology Management*, Special Issue, 23-43.