EFFICIENT IMAGE ENCRYPTION ALGORITHM USING REGION-WISE GENERALIZED SINGULAR VALUE DECOMPOSITION

V. SURESH BABU[1], V.R. VIJAYKUMAR[2]
[1, 2]Department of Electronics and Communication Engineering,
[1] Christ the King Engineering College Coimbatore, Tamilnadu, India.
[2] Anna university Regional Campus Coimbatore, Tamilnadu, India.
E-mail: sureshvece@gmail.com; vr.vijaykumar@gmail.com

Abstract.

A new method for image encryption using Generalized Singular Value Decomposition (GSVD) is proposed in this paper. Also, the traditional confusion and diffusion based framework concept is not used in this paper, to reduce the time constraint. Here, the encryption method uses the element-wise GSVD. The GSVD decomposes any matrix of data into three portions with respect to another data matrix of same size. The secret image and the self generated random value are inputs for GSVD module and it decomposes the inputs into five different matrices. From the outputs of GSVD module, the ciphered image and the key are derived from the obtained decomposed data in a specific format. The self generated random value is a synchronous model. The separate key is not provided for this encryption method. The key size depends on the size of the ciphered image matrix. The generated ciphered image and the key are highly sensitive and robust. Because of that, proposed scheme is a less time consuming and less complex encryption and decryption method. Also, this work provides very good key sensitivity which is observed from the experiments, that means even a very small change in the key forbids the secret image to be perceived. The proposed work is compared with the state-of-art techniques using the quantitative parameters Encryption time, Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Correlation Coefficient, Information Entropy and Key Space.

Keywords: ***Image Encryption, Generalized Singular Value Decomposition (GSVD), Synchronous Random Value Generator***
DOINumber:10.14704/nq.2022.20.8.NQ44630 **NeuroQuantology2022;20(8):6033-6050**

1. Introduction

In this information era, the information security is the predominant problem in all aspects of digital communication. In order to overcome this problem, there are many techniques available. And, still there are difficulties in achieving reliability in digital data transmission and storage. From this context, the expectation on any secret image sharing scheme is, that it has to prevent secret image data loss or modification during transmission or storage. The efficiency of the conventional encryption algorithms like data encryption standard (DES), advanced encryption standard (AES) are not satisfactory. Beyond those conventional encryption methods, there are various other types of image encryption methods derived, for example secret image sharing scheme based on singular value decomposition method (SVD) [4], [6], [8], [10], [12], [13],

fractional Fourier transform (FrFT) [6], [12], [32], fractional discrete cosine transform (FrDCT), [15], elliptic curve, [22], [23], steganography, [38], chaotic, [3], [16], [30], [31], [36], threshold, [24], [26], [34], Gyrator & Fresnel transforms, [14], public key encryption, [2], logistic map, [25], arithmetic, [27], pixel-wise image scrambling, [35], Quaternion, [33], and so on. Here, most encryption algorithms use confusion-diffusion method (confusion operation changes the pixel position and diffusion operation changes the pixel values) [1]. In confusion-diffusion method the process undergoes many numbers of rounds to achieve high security. This makes the encryption method more complex and time consuming. The time consumption and encryption design complexity are also significant factors to be a good image encryption algorithm.

To reduce time and design complexity, the number of rounds in confusion and diffusion method is used in few papers.

In order to overcome the general problems like more encryption time, computational complexity, less pixel wise correlation of ciphered image etc., the proposed method introduces a decomposition method based on generalized singular value decomposition (GSVD) [17] – [21]. Here, to avoid confusion-diffusion method plain image is decomposed with respect to any key image which is commonly shared to sender and receiver as shown in figure 1. This method just involves GSVD decomposition [28] [29] [40] which provide less time consumption and design architecture is simple. The experimental result shows very good efficiency of the method and also ensures more security. This method is robust against many different types of attacks which are discussed in results in later sections. Here, the decryption algorithm consumes very less time because of its simple structure. However, this method provides sensitive keys. Here, in this paper, all the above listed features are demonstrated clearly. The proposed algorithm contributes the following satisfactory feature:

[1] A novel GSVD based image encryption reduces the encryption time of the algorithm by avoiding the conventional confusion-diffusion method.
[2] The proposed scheme provides a satisfactory performance against the differential attack. That is, the sensitivity to slight change in the secret image is improved.
[3] The proposed algorithm is robust against noise attacks and is demonstrated (for Gaussian and impulse noise).
[4] The proposed method is robust against brute-force attack by providing a very large key space.
[5] The satisfactory key Sensitivity can be achieved by our proposed image encryption scheme.

This paper is organized as follows: Section 2 discuss about the existing methods, Section 3 explains about the mathematical model and few characteristic features of GSVD. Section 4 describes the proposed image encryption method with algorithm, flowchart, and diagram for both encryption and decryption. In section 5 the simulated results, comparisons and security analysis are presented. Section 6 presents the conclusion of this paper.

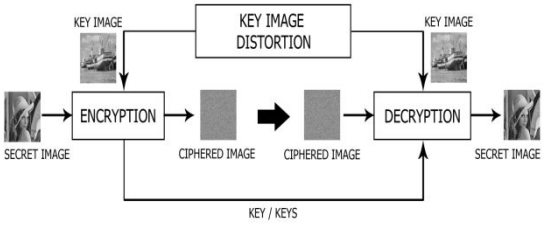


Figure 1: Proposed General Secret Image Sharing Scheme

2. RELATED WORKS

In this work, few state of art techniques are discussed as related works. Those state of art works are as follows.

Hegui Zhu et al. [11] proposed a 2D chaotic map called 2D Logistic-modulated-Sine-coupling-Logistic Chaotic Map Image Encryption Algorithm (LSMCL-IEA). This method provided good time performance, low correlated pixel ciphered image and reduced design complexity. Hegui Zhu et al. achieved this by reducing number rounds in the usual confusion-diffusion method. Here, only two rounds of permutation are allowed in LSMCL-IEA method. Also, this method provided good key sensitivity.

Roayat Ismail Abdelfatah [3] proposed a double-chaotic image encryption method. In this method, the hash value of the plain image is derived using SHA-512. The derived hash value is bitwise rotated to perform the first round of permutation. This method provides two rounds of permutation by repeating this process. This paper also achieved good security and efficiency, compared to previous methods. The less number of permutation makes this algorithm faster comparatively. Here, the double chaotic pseudo random generator (DCPG) and simple XOR operations are used, to increase the security in spite of reduced number of permutation operation. The DCPG requires three values of control parameters which are shared secret key. The DCPG is just the combination of both tent and Chebyshev chaotic algorithm. Also, it is faster than the other previous confusion-diffusion based image encryption method.

Changzhi Yu et al. [10] proposed a Singular Value Decomposition (SVD) based image encryption method. In this method, the secret image is decomposed into three different matrixes. After SVD, the logistic-tent-sine system (LTSS) is used to chaotic map the decomposed segments of the secret image. This method has less a very design complexity and consumes less time. It produces pixel wise less correlation ciphered image with high security. This secret image sharing scheme provides identity authentication and compression facility also.

Yanjie Songet el. [1] proposed the key-substitution architecture (KSA) scheme which is used as image encryption algorithm. This paper is mainly overcoming the time consumption and complex design problem in confusion-diffusion based image encryption algorithm. The only one round in any conventional confusion-diffusion based image encryption algorithm, the security is comparatively inadequate and the efficiency is much lesser. This KSA image encryption algorithm (KSA-IEA) has two stages in it encryption operation. The first stage is key scheming and the second stage is substitution in KSA-IEA. This key scheming method generates a ciphered image from a plain image using a chaotic algorithm based on initial key. In substitution the items of the histogram of the outcome of key scheming is scrambled to provide resistance against statistical analysis attacks.

3. Fundamental Knowledge

Generalized Singular Value Decomposition (GSVD)

Let us assume the any matrices be A and B of size m×n and l×n respectively. All elements of A and B belongs to real number. Then using GSVD [21], matrix A and B can be decomposed as follows:

$$[U,W,V^T,\varphi,\psi]=GSVD(A,B)$$

Where, $A=U\varphi V^T$ and $B=W\psi V^T$ (1)

Where, φ and Ψ are diagonal matrix of size m×r and l×r respectively.

U, W and V are orthogonal matrix of size m×m, l×l and r×r respectively.

To analyse GSVD [17], let us consider, $P_A=A^TA$; $P_B=B^TB$; now $P=P_A+P_B$.

(2)

Decomposing P with SVD gives, $P=O\Omega O^T$; where O is a matrix of real number of size n×r and $\Omega=\mathrm{diag}(w_1,w_2,...,w_r);\ w_1\geq....\geq w_r\succ 0$. The k-th column of matrix O is a Eigen vector of P corresponding to Eigen value w_k^2 fork= 1,2,…,r. Then, we know,

$Q_A=\Omega^{-1}O^TP_AO\Omega^{-1}$ and $Q_B=\Omega^{-1}O^TP_BO\Omega^{-1}$ (3)

$$Q_A + Q_B = \Omega^{-1}O^T(P_A + P_B)O\Omega^{-1}$$
$$= \Omega^{-1}O^T PO\Omega^{-1}$$
$$= \Omega^{-1}O^T O\Omega^2 O^T O\Omega^{-1}$$
$$Q_A + Q_B = I_r \quad (4)$$

Where, I_r is identity matrix of size r×r.

The spectral decomposition of Q_A and Q_B are given by,

$$Q_A = T\varphi^2 T^T; \varphi = diag(\varphi_1, \varphi_2, .., \varphi_r); \quad (5)$$
$$\varphi_i \geq 0; i = 1, 2, .., r$$

$$Q_B = T\psi^2 T^T; \psi = diag(\psi_1, \psi_2, .., \psi_r); \quad (6)$$
$$\psi_i \geq 0; i = 1, 2, .., r$$

$$\varphi_i^2 + \psi_i^2 = 1; \varphi_i \geq 0; \psi_i \geq 0; i = 1, 2, .., r \quad (7)$$

In GSVD [21], $V = O\Omega T$. (8)

Therefore, the matrices U and W are,

$U\varphi = AO\Omega^{-1}T$; and $W\psi = BO\Omega^{-1}T$. (9)

These equation and understanding of GSVD supports the key generation and image synthesis of both cover and secret image.

4. PROPOSED METHODOLOGY

4.1. Encryption Process

Let us assume 'A' size (m*n) be the secret image and 'B' of size (m*n) be the matrix of 8-bit random value. The proposed image encryption method includes GSVD tool for the efficient encryption of the secret image. First, both the secret image 'A' and the generated random values 'B' are decomposed element wise with respect to each other. In this method, Combined Multiple Recursive Synchronous random value generator is used. The random value generator can only be synchronised by seed value. Each element of secret image and its corresponding random value is decomposed into five different element for each element of A and B separately. This GSVD decomposition is actually explained in equation (1), that is, $A_{ij} = U_{ij}\varphi_{ij}V_{ij}$ and $B_{ij} = W_{ij}\psi_{ij}V_{ij}$. Here, the A_{ij} is $(i, j)^{th}$ pixel element of the secret image. The B_{ij} is generated random value matrix, and (i, j) denotes the position of the pixel of the corresponding element.

The encryption and key generation of the proposed method is described through the figure 2. Using secret image, A and random value matrix, B are decomposed element wise using GSVD into five matrix components as discussed in equation (1). In those matrix components each elements of 'U' & 'W' are valued as '1' always and the elements of 'ϕ' & 'ψ' are carry values ranges 0 to 1. The matrix 'ψ' is a part of random value matrix. The elements of matrix 'ψ' is quantized to 8-bit unsigned integer and is assigned as ciphered image. The seed value of the random value generator is used as key for the encryption scheme too. The size of the encryption key is 256 bits.

Encryption Procedure:

Step 1: Assign the secret image, A, the key value to generate random values and the random value matrix, B.

Step 2: The Combined Multiple Recursive Synchronous random value generator is initiated using the seed value mentioned in step 1.

Step 3: Generate the matrices 'ψ' by applying element wise GSVD on A and B.

$$[U, W, V^T, \varphi, \psi] = GSVD(A, B)$$

Step 4: The values of the elements of matrix 'U' and 'W' are '1' or '-1' for the element wise GSVD operation.

Step 5: The value of 'ψ' matrix is converted to 8-bit unsigned values.

Step 6: The converted matrix is assigned as the cipher image.

Step 7: The seed value is set as key for the encryption scheme.

*e*ISSN1303-5150

Here, followed by this procedure a general pseudo code or algorithm is shared.

Algorithm of the encryption procedure:

Inputs: Secret image, A, Seed value for the random value generator

Outputs: Ciphered image, Encryption Key

1: Assign the initial seed value for the combined multiple recursive synchronous random value generator.

2: Assign the secret image, A.

3: The matrix, B of the size of secret image is generated using random value generator.

4: For i=1:m

5: For j=1:n % (m,n) is size of the secret image

6: $[U_{ij}, W_{ij}, V_{ij}^{T}, \varphi_{ij}, \psi_{ij}] = GSVD\left(A_{ij}, B_{ij}\right)$ %Applied Element wise GSVD on A and B

7: Ciphered image, $C_{ij} = round\,|\psi_{ij} * 255|$

8: End

9: End

10: Return Ciphered image, C

11: Return Seed value = Encryption Key

For clarity, the general pseudo code or algorithm is provided with required explanation.

3.2 Decryption Process

Here, we discuss the reverse process of encryption procedure in section 4.1 to decrypt and synthesis secret image. The decryption module is initially provided with ciphered image, C, and Encryption key. Using this key random value is generated and random valued matrix, A is generated. By using the key, ciphered image, C is decrypted as illustrated in figure 3.

In decryption module, the received key is used to synchronize the random value generator. The elements of received ciphered image will be converted to 8-bit value range between 0 and 1. For all values of $0 \le i \le m$, $0 \le j \le n$ the value of U_{ij} & W_{ij} is 1. So, for all values of $0 \le i \le m$, $0 \le j \le n$, $\overline{V_{ij}} = \frac{B_{ij}}{\overline{\psi_{ij}}}$ is calculated using equation (1). $\overline{\psi}$ is derived from the received ciphered image,C. By applying in equation (7) to derive $\overline{\varphi_{ij}} = |\sqrt{1-\overline{\psi_{ij}}^{2}}\,|$. From this $\overline{\varphi}$ is derived. By knowing U, $\overline{\varphi}$ & $\overline{V}$ the secret image is synthesized. The synthesized secret image is $\overline{A} = \mathrm{round}(|\,\overline{\varphi} * \overline{V}\,|)$.

Decryption Procedure:

Step 1: Receive the ciphered image, C

Step 2: Encryption key is received.

Step 3: Using 'Key' random valued 8-bit unsigned matrix, B is generated.

Step 4: Recovered ψ is $\overline{\psi} = \left|\frac{C}{255}\right|$.

Step 5: Using $\overline{\psi}$ and B , $\overline{V}$ is derived.

Step 6: Using $\overline{\psi}$, φ is derived which is denoted as $\overline{\varphi}$.

Step 7: As the elements of matrices U and W are unity, using matrices $\overline{\varphi}$ and $\overline{V}$ the secret image is derived and it is denoted as $\overline{A}$.

*e*ISSN1303-5150

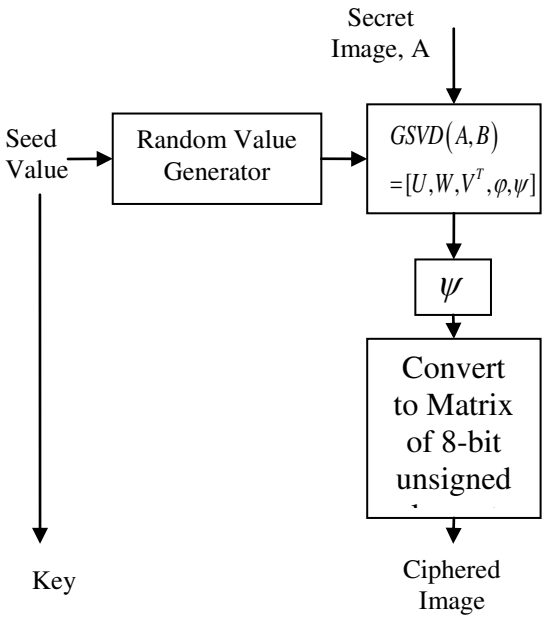


Figure 2: Image Encryption & Key Generation

Algorithm of the decryption procedure:

Inputs: Ciphered image, C, Seed value for the random value generator

Outputs: Synthesized secret image

1: Assign the initial seed value for the combined multiple recursive synchronous random value generator. 6038

2: Assign the Ciphered image, C.

3: The matrix, B of the size of secret image is generated using random value generator.

4: $\overline{\psi} = \left| \frac{C}{255} \right|$

5: For i=1:m

6: For j=1:n % (m,n) is size of the secret image

7: $\overline{V_{ij}} = \frac{B_{ij}}{\overline{\psi_{ij}}}$

8: $\overline{\varphi_{ij}} = \left| \sqrt{1 - \overline{\psi_{ij}}^2} \right|$

9: $\overline{A}_{ij} = \text{round}(|\overline{\varphi_{ij}} * \overline{V_{ij}}|)$

10: End

11: End

12: Return Synthesized secret image, $\overline{A}$

For clarity, the general pseudo code or algorithm is provided with required explanation.

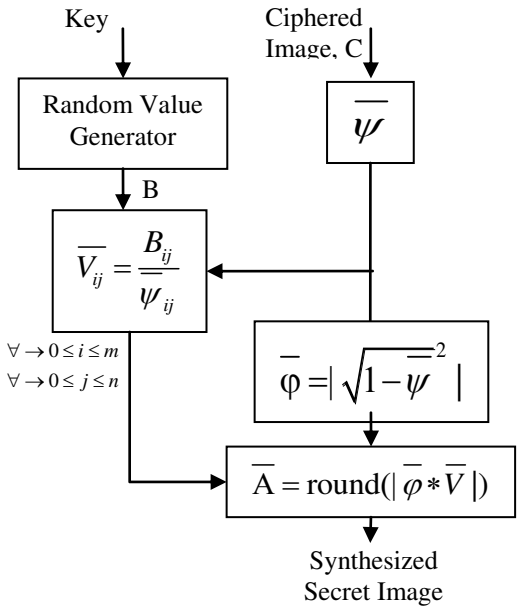


Figure 3: Secret Image Synthesis

5. Simulation and Security Analysis

In this section, we present a simulation results and security comparison between other recent state of art image encryption algorithms. Those algorithms compared with proposed method are CMT-IEA [9], LSMCL-IEA [11], CS-IEA [5], HF-IEA [7] and KSA-IEA [1]. The evaluation of the proposed algorithm with the quantitative methods is presented in this section. The simulation outputs, speed analysis, security against differential & noise attacks, correlation analysis, information entropy, key space and key sensitivity are the factors analysed with some quantitative techniques. Here, the image encryption scheme is performed on the grey-scale images. It scores the satisfactory numbers in the quantitative parameters (which are discussed as follows).

The implementation tool configuration on which the simulation performed is a personal computer with an Intel CORE i7-6500u CPU (runs at 2.50 GHz and 8 GB RAM). The images chose here were grey-scale with resolution 512*512.The initial seed value for the random value generator is set as '1' (and it depends on the size of secret image).

5.1. Simulation Results

Here, a set of 20 images are used in the simulation process for different set of experiments and result analysis as mentioned in the table 1. For the proposed image encryption scheme general simulation we use four familiar images (grayscale). They are sample-1, sample-2, sample-3 and sample-4. All these images have resolution of about 512*512. The simulation results show a satisfactory performance on resisting statistical attack. However, the decrypted image obtained from the ciphered image using proposed scheme is lossless. The simulation result images are displayed in the fig. 4, fig. 5, fig. 6, fig. 7 and fig. 8. In the fig. 4, four original images are displayed, sample-1, sample-2, sample-3 and sample-4 in (a), (b), (c) and (d) respectively. In fig. 5, the ciphered images using proposed encryption scheme on the corresponding original images in fig. 4. The images decrypted from the ciphered images in fig. 5 are displayed in fig. 6 respectively. In fig. 7(a,b,c,d), the histograms of the original images in fig. 4(a,b,c,d) are displayed respectively. In fig. 8, the histograms of the corresponding ciphered image shown in fig. 5 are displayed. So, the performance of the encryption method is satisfactory for various images. The simulation results find that the histogram of the ciphered image is uniformly distributed which shows the randomness of the values of the encrypted image.

5.2. Speed Analysis

The speed analysis refers the execution time of the image encryption scheme. This execution time consumption is an important factor for any image encryption algorithm. Here, we compared our proposed method with few recent works. They are CMT-IEA, [9], LSMCL-IEA, [11], CS-IEA, [5], HF-IEA, [7] and KSA-IEA, [1]. Here, to analyse the speed of the image encryption algorithm, we calculated the time consumed by the algorithm to encrypt the colour and grayscale image of size 512*512.

For the simulation of the scheme, we used Matlab 2019a software in a computer with the same specification as mentioned in beginning this section. The results are displayed in the table 1 and table 2. This comparison provides enough evident that the proposed scheme have a satisfactory speed on most cases.

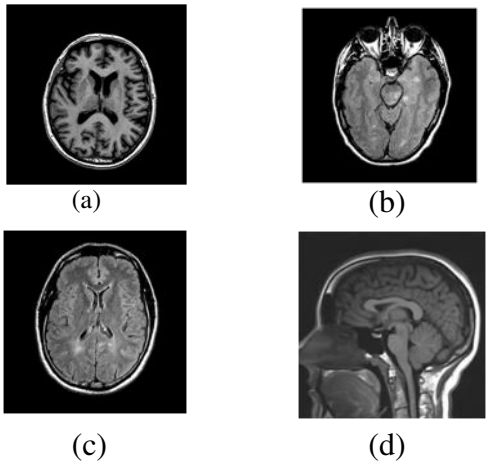


Fig. 4.*Chosen Secret Images is CT scan of four different types of greyscale Brain image (a) Sample-1; (b) Sample-2; (c) Sample-3; (d) Sample-4*

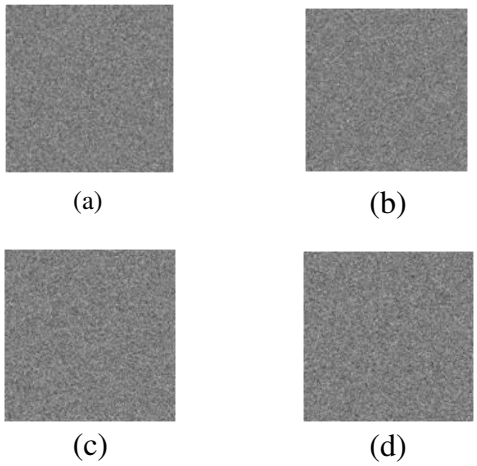


Fig. 5.*Ciphered Image of (a) Sample-1; (b) Sample-2; (c) Sample-3; (d) Sample-4*

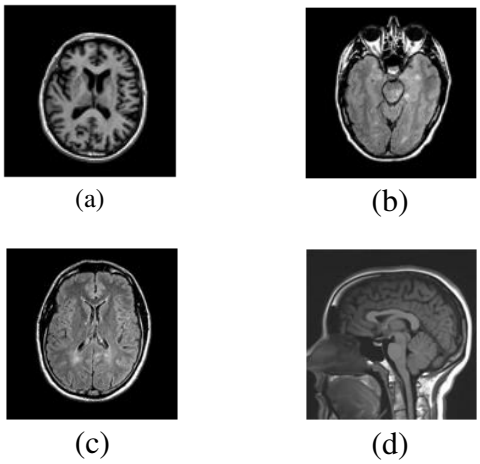


Fig. 6.*Decrypted and restored Secret Image (a) Sample-1; (b) Sample-2; (c) Sample-3; (d) Sample-4*

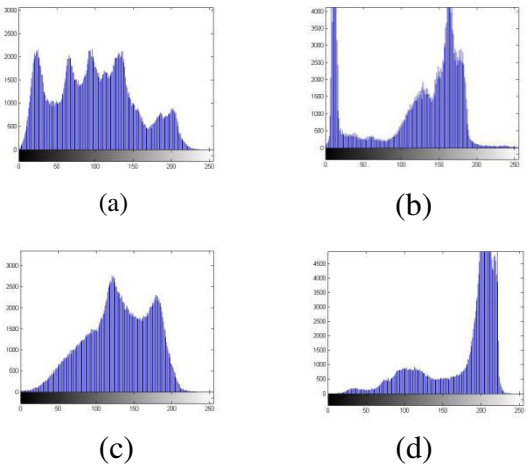


Fig. 7.*Histogram of original Secret Image (a) Sample-1; (b) Sample-2; (c) Sample-3; (d) Sample-4*

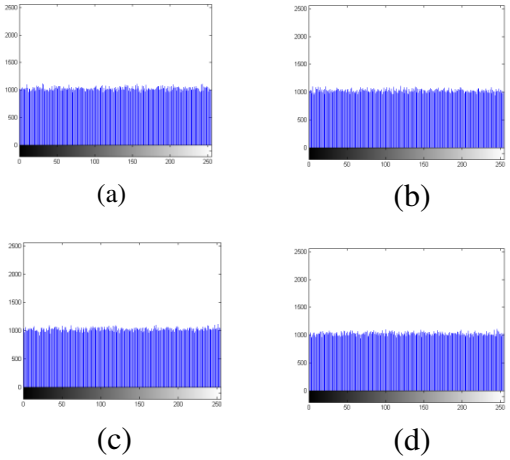


Fig. 8.*Histogram of Ciphered Image (a)Sample-1; (b) Sample-2; (c) Sample-3; (d) Sample-4*

5.3. Differential Attack

The image encryption scheme is robust against the differential attack. It means, if

even the small change of value in the secret image produces totally different ciphered image. This property can be analysed quantitatively using two parameters, they are, the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). These parameters evaluate the ability of any encryption scheme to resist the differential attack. The NPCR and UACI is defined as follows in equation (13).

$$\begin{cases} NPCR = \dfrac{\sum_{ij} D(i,j)}{M*N} * 100\% \\ UACI = \dfrac{1}{M*N}\left[\sum_{i,j} \dfrac{|C_1(i,j) - C_2(i,j)|}{255}\right] * 100\% \end{cases} \quad (13)$$

Where the $C_1(i,j)$ and $C_2(i,j)$ are the value of pixel in the position (i,j) of two different ciphered image. The C_1 is the ciphered image of actual secret image and C_2 is the ciphered image of slightly changed secret image. The M*N denotes the resolution of the image. Then, the D is a matrix depends on C_1 and C_2, that is if $C_1(i,j) \neq C_2(i,j)$, then D(i,j)=1 and otherwise D(i,j)=0.

In table 3, table 4 & table 5 the observed values of the NPCR and UACI of the proposed scheme are compared with the five recent methods. Usually, to resist chosen /known plaintext attack, any satisfactory image encryption algorithm should be sensitive to small changes in the plain-image. Also, in table 5, the values of NPCR and UACI of proposed scheme with other three recent methods for colour images. From the observation, the above mentioned data clearly depicts that the proposed image encryption scheme is very sensitive to the change in plain text.

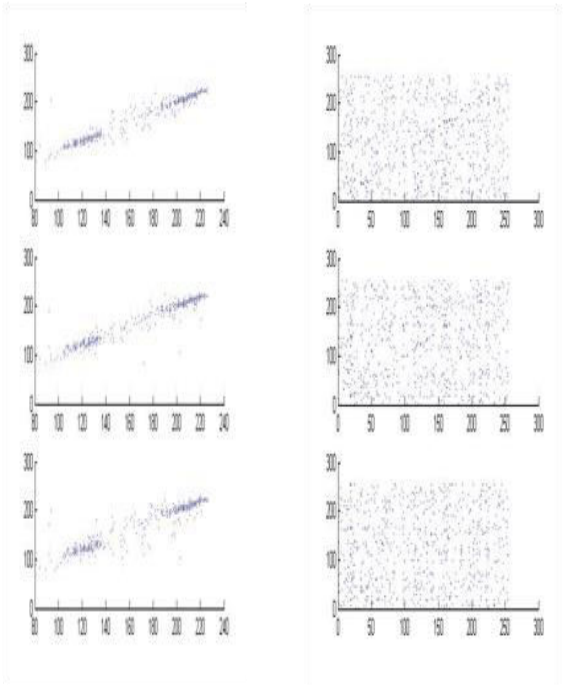
5.4. Correlation Analysis

The correlation analysis is generally observed with very high value in original secret image. Here, the correlation analysis actually means the pixel wise similarity of any image in horizontal, vertical and diagonal direction. It is clearly defined in equation (14).

$$\begin{cases} \rho = \dfrac{E[(x - E(x))(y - E(y))]}{D(x)D(y)} \\ E(x) = \dfrac{1}{\omega}\sum_{i=1}^{\omega} x_i \\ D(x) = \dfrac{1}{\omega}\sum_{i=1}^{\omega} [x_i - E(x)]^2 \end{cases} \quad (14)$$

Where the operator E[.] is expectation and D[.] is variance. The variable x and y represents the actual set of values of the ciphered image and the shifted (in horizontal, vertical and diagonal directions) set of values of the ciphered image. Any good image encryption scheme should produce a ciphered image with less correlation coefficient (ρ). The correlation coefficient always varies between the values [0,1]. Here, we used twenty grayscale images and six colour images for the correlation analysis. In fig. 9 and fig. 10, we present the scatter plot of the secret images for the horizontal, vertical and diagonal direction correlation coefficient values.

In table 6 and table 7, the observed values of the correlation coefficient of the plain image and ciphered image encrypted using proposed scheme are compared with the five other recent schemes for grayscale image of size 512*512. The same kind of comparison is applied for a colour image too in table 7.



(a),(b) & (c) (d), (e) & (f)

Fig. 9.*Correlation Coefficient of Secret Image Sample-1 and its Corresponding Ciphered Image; (a) Horizontal Correlation of Sample-1 Image; (b) Vertical Correlation of Sample-1 Image; (c) Diagonal Correlation of Sample-1 Image; (d) Horizontal Correlation of Ciphered Sample-1 Image; (e) Vertical Correlation of Ciphered*
Sample-1 Image; (f) Diagonal Correlation of Ciphered Sample-1 Image

5.5. Information Entropy

The randomness of the encrypted image can be evaluated by the criterion information entropy. Generally, the cipher-image should be highly random. The value of information entropy is high for more random ciphered image. The information entropy is defined as

,

$$H(x) = \sum_{i=0}^{MN-1} P(x_i) \log \frac{1}{P(x_i)} \qquad (15)$$

where, x_i is the i-th pixel value in the ciphered image of size M*N and $P(x_i)$ is the probability of x_i . In table 8, the ciphered image of twenty different grayscale images are evaluated for information entropy, using the proposed scheme and other five recent image encryption scheme.

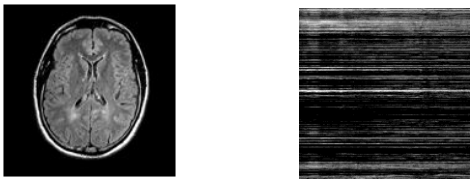
In table 9, few colour images are considered for the comparison of information entropy values of its encrypted images. Usually, this information entropy is a value which lies between 0 and 8. From the comparison table 8 and table 9, we clearly know that the proposed GSVD based IES is a good scheme on this perspective too. That is, it provides high randomness in its encrypted image.

5.6. Key Space and Key Sensitivity

For a good image encryption scheme, the key space size should be atleast 128 bit. This is a sufficient value to resist burte-force

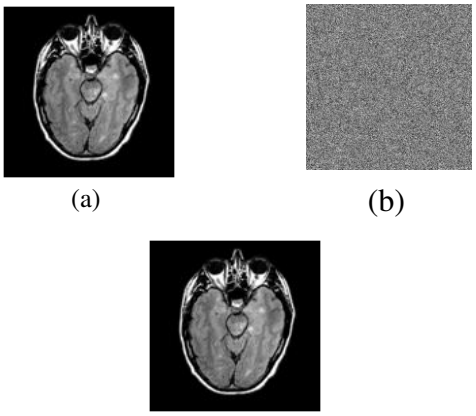
attack. In our proposed scheme, the key space size is 512 bit.

To check the sensitivity of the key of the proposed scheme, a slight change in the value of key is applied to decrypt the image. The result of this simulation is shown in fig. 10. The decrypted image does not contain any information of the secret image. Here, we chose a grayscale image for analysis. That image is Lena.tif and its resolution is 512*512. The decrypted image with the slightly changed key is totally degraded and there is no influence of the secret image.



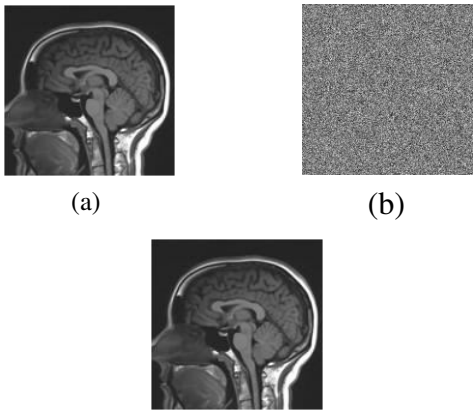
(a) (b)

Fig. 10.*Simulation for the Key Sensitivity (a) Sample-3 Image; (b) Decrypted Image With Slight Change in the Key*



(a) (b) (c)

Fig. 11.*Simulation of the Gaussian Noise Attack (a) Sample-2 Image; (b) Gaussian Noise Added Cipher-Image; (c) Decrypted Image*



(a) (b) (c)

Fig. 12.*Simulation of the Impulse Noise Attack (a) Sample-4 Image; (b) 'Salt & Pepper' Noise Added Cipher-Image; (c) Decrypted Image*

5.7. Noise Attack

Any good image encryption algorithm should be very robust against the noise attack. To check the robustness of the proposed scheme against the noise attack, we add the Gaussian noise (with mean as '0' and variance as 0.1) to the cipher-image. Then, the simulation decrypts that "noise added" cipher-image. This simulation results are present in the fig. 11, which proves the ability of the proposed scheme against noise attack. In fig. 12, the simulation results of the effect of 'salt and pepper' noise on the ciphered image before decryption is displayed. The ciphered image is corrupted with the noise density of 0.2. Then, synthesized output image is display in fig. 12 (c). The performance of the scheme is good on both Gaussian and 'salt & pepper' noises.

6. Conclusion

The element wise generalized singular value decomposition (GSVD) based encryption scheme is proposed in this paper. There are five state-of-art encryption schemes namely CMT-IEA, LSMCL-IEA, CS-IEA, HF-IEA and KSA-IEA are compared with the proposed work. From the simulation results and discussion on that topic, the performance of the proposed scheme is satisfactory. The primary advantage of the proposed scheme less complex and fast method when compared to the conventional confusion-diffusion based methods. So, from the result analyses and comparison tables of section V, the speed of the encryption method, the robustness of the scheme against differential attack (by NPCR and UACI), robustness against noise attack (by fig. 11 and fig. 12), key space and key sensitivity (by fig. 10) are performing better than the other methods. This GSVD based image encryption method may provide space for further enhancements in the field of the VLSI implementation feasibilities.

References

1. Song, Y., Zhu,Z., Zhang, W., et al.:'Efficient and secure image encryption algorithm using a novel key-substitution architecture',IEEE Access,2019,7, pp. 84386– 84400
2. Xie, D.: 'Public key image encryption based on compressed sensing', IEEE Access, 2019, 7, pp. 131672–131680
3. Abdelfatah, R.I.: 'A new fast double-chaotic based Image encryption scheme',Multimed. Tools Appl., 2019, pp. 1–19
4. Bhatnagar, G., Jonathan Wu, Q.M.: 'Selective image encryption based on pixels of interest and singular value decomposition', Digit. Signal Process. A Rev. J., 2012, 22, (4), pp. 648–663
5. Pak, C., Huang, L.: 'A new color image encryption using combination of the 1D chaotic map', Signal Processing, 2017, 138, pp. 129–137
6. Singh, P., Raman, B., Misra, M.: 'A secure image sharing scheme based on SVD and fractional Fourier transform', Signal Process. Image Commun., 2017, 57, pp. 46–59
7. Amina, S., Mohamed, F.K.: 'An efficient and secure chaotic cipher algorithm for image content preservation', Commun. Nonlinear Sci. Numer.Simul., 2018, 60, pp. 12–32
8. Kumar, M., Vaish, A.: 'An efficient encryption-then-compression technique for encrypted images using SVD', Digit. Signal Process. A Rev. J., 2017, 60, pp. 81–89
9. Hua, Z., Zhou, Y., Pun, C.M., et al.: '2D Sine Logistic modulation map for image encryption', Inf. Sci. (Ny)., 2015, 297, pp. 80–94
10. Yu, C., Li, H., Wang, X.: 'SVD-based image compression, encryption, and identity authentication algorithm on cloud', IET Image Process., 2019, 13, (12), pp. 2224–2232
11. Zhu, H., Zhao, Y., Song, Y.: '2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map for Image Encryption', IEEE Access, 2019, 7, pp. 14081–14098
12. Girija, R., Singh, H.: 'A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition', Opt. Quantum Electron., 2018, 50, (5), pp. 50–250

13. Girija, R., Singh, H.: 'An asymmetric cryptosystem based on the random weighted singular value decomposition and fractional Hartley domain', Multimed. Tools Appl., 2019, pp. 1–19
14. Khurana, M., Singh, H.: 'Asymmetric optical image triple masking encryption based on Gyrator and Fresnel transforms to remove Silhouette problem', 3D Res., 2018, 9, (3), pp. 1–17
15. Liang, Y.R., Xiao, Z.Y.: 'Image Encryption Algorithm Based on Compressive Sensing and Fractional DCT via Polynomial Interpolation', Int. J. Autom. Comput., 2018, pp. 1–13
16. Ponuma, R., Amutha, R., Aparna, S., et al.: 'Visually meaningful image encryption using data hiding and chaotic compressive sensing', Multimed. Tools Appl., 2019, 78, (18), pp. 25707–25729
17. Friedland, S.: 'A new approach to generalized singular value decomposition', SIAM J. Matrix Anal. Appl., 2006, 27, (2), pp. 434–444
18. Wang, J.: 'Computing the CSD and GSVD', Semant. Sch., 2004, (1), pp. 1–21
19. Vandewalle, J., Callaerts, D.: 'Singular value decomposition: A powerful concept and tool in signal processing', Math. Signal Process., 1990, pp. 539–560
20. Hansen, P.C.: 'Relations between SVD and GSVD of Discrete regularization problems in standard and general form', Linear Algebra Appl., 1990, 141, pp. 165–176
21. Hansen, P.C.: 'Regularization, GSVD and truncated GSVD', BIT Number. Math., 1989, 29, (3), pp. 491–504
22. Luo, Y., Ouyang, X., Liu, J., et al.: 'An image encryption method based on elliptic curve Elgamal encryption and chaotic systems', IEEE Access, 2019, 7, pp. 38507–38522
23. Zhang, X., Wang, X.: 'Digital image encryption algorithm based on elliptic curve public cryptosystem', IEEE Access, 2018, 6, pp. 70025–70034
24. Kabirirad, S., Eslami, Z.: 'A (t, n)-multi secret image sharing scheme based on Boolean operations', J. Vis. Commun. Image Represent., 2018, 57, pp. 39–47
25. Ismail, S.M., Said, L.A., Radwan, A.G., et al.: 'Generalized double-humped logistic map-based medical image encryption', J. Adv. Res., 2018, 10, pp. 85–98
26. Yan, X., Lu, Y., Liu, L., et al.: 'Partial secret image sharing for (k,n) threshold based on image inpainting', J. Vis. Commun. Image Represent., 2018, 50, pp. 135–144
27. Meghrajani, Y.K., Desai, L.S., Mazumdar, H.S.: 'Secure and efficient arithmetic-based multi-secret image sharing scheme using universal share', J. Inf. Secur. Appl., 2019, 47, pp. 267–274
28. Chen, F., Wong, K.W, Liao, X., et al.: 'Period distribution of generalized discrete Arnold cat mapfor N=p^e', IEEE Trans. Inf. Theory, 2012, 58, (1),pp. 445–453
29. Chen, F., Wong, K.W., Liao, X., et al.: 'Period distribution of the generalized discrete Arnold cat map for N = 2^e', IEEE Trans. Inf. Theory, 2013, 59, (5), pp. 3249–3255
30. Zhang, X., Wang, L., Zhou, Z., et al.: 'A chaos-based image encryption technique utilizing Hilbert curves and H-fractals', IEEE Access, 2019, 7, pp. 74734–74746
31. Belazi, A., Talha, M., Kharbech, S., et al.: 'Novel medical image encryption scheme based on chaos and DNA encoding', IEEE Access, 2019, 7, pp. 36667–36681
32. Tao, R., Meng, X.Y., Wang, Y.: 'Image encryption with multiorders of fractional Fourier transforms', IEEE Trans. Inf. Forensics Secur., 2010, 5, (4), pp. 734–738
33. Dzwonkowski, M., Papaj, M., Rykaczewski, R.: 'A new quaternion-based encryption method for DICOM images', IEEE Trans. Image Process., 2015, 24, (11), pp. 4614–4622
34. Bao, L., Yi, S., Zhou, Y.: 'Combination of Sharing Matrix and Image Encryption for Lossless (k,n)-Secret Image Sharing', IEEE Trans. Image Process., 2017, 26, (12), pp. 5618–5631
35. Li, C., Lin, D., Lu, J.: 'Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits', IEEE Multimed., 2017, 24, (3), pp. 64–71

6046

36. Ge, R., Yang, G., Wu, J., Chen, Y., Coatrieux, G., Luo, L.: 'A Novel Chaos-Based Symmetric Image Encryption Using Bit-Pair Level Process', IEEE Access, 2019, 7, pp. 99470–99480
37. Sharma, V.K., Srivastava, D.K., Mathur, P.: 'Efficient image steganography using graph signal processing', IET Image Process., 2018, 12, (6), pp. 1065–1071
38. Qin, Y., Zhang, Y.: 'Information encryption in ghost imaging with customized data container and XOR operation'IEEE Photonics J., 2017, 9, (2)
39. Ramakrishnan.S., Gopalakrishnan.T., et el.: 'Awavelet based hybrid SVD algorithm for digital image watermarking', Signal and Image Process. :An Internat. Jour., 2011, 2, (3), pp. 157-174
40. Wu, L., Deng, W., Zhang, J., He, D.: 'Arnold transformation algorithm and anti-Arnold transformation algorithm', 1st Int. Conf. Inf. Sci. Eng. ICISE 2009, 2009, pp. 1164–1167

Table1. Encryption time (s) comparison of six image encryption algorithms for grayscale images

No.	Image	CMT-IEA [9]	LSMCL-IEA [11]	CS-IEA [5]	HF-IEA [7]	KSA-IEA [1]	GSVD-IEA
1	Sample-1	1.5012	3.5385	0.8111	16.3479	0.3556	**0.3334**
2	Sample-2	1.4671	2.7383	0.7684	16.2074	0.3360	**0.3352**
3	Sample-3	1.4708	2.7528	0.7767	16.1032	0.3379	**0.3329**
4	Sample-4	1.4472	2.7352	0.8031	16.1701	0.3336	**0.3299**
5	Sample-5	1.4491	2.8154	0.7622	16.3447	0.3329	**0.3282**
6	Sample-6	1.4423	2.7407	0.7683	16.0454	0.3626	**0.3398**
7	Sample-7	1.4986	2.7331	0.8082	16.2089	0.3288	**0.3378**
8	Sample-8	1.4790	2.7564	0.7714	16.2084	0.3367	**0.3321**
9	Sample-9	1.4378	2.7406	0.7999	16.0721	0.3362	**0.3311**
10	Sample-10	1.5116	2.7648	0.7843	16.1259	0.3403	**0.3343**
11	Sample-11	1.4859	2.7686	0.7866	16.1279	0.3405	**0.3329**
12	Sample-12	1.4529	2.7997	0.7712	16.1025	0.3254	**0.3219**
13	Sample-13	1.5269	2.7111	0.7889	16.2597	0.3505	**0.3392**
14	Sample-14	1.4429	2.8555	0.7940	16.2228	0.3494	**0.3398**
15	Sample-15	1.4530	2.8402	0.7800	16.1139	0.3321	**0.3230**
16	Sample-16	1.4529	2.7652	0.7811	16.1994	0.3335	**0.3290**
17	Sample-17	1.4586	2.7568	0.7729	16.1495	0.3364	**0.3231**
18	Sample-18	1.4691	2.7559	0.7721	16.1457	0.3311	**0.3302**
19	Sample-19	1.4924	2.7713	0.7665	16.1287	0.3449	**0.3315**
20	Sample-20	1.4987	2.8145	0.8119	16.1248	0.3132	0.3243

6047

Table 2. Encryption time (s) comparison of four image encryption algorithms for color image

No.	Image	LSMCL-IEA [11]	CS-IEA [5]	KSA-IEA [1]	GSVD-IEA
1	Airplane	8.9538	2.3101	0.8774	**0.8559**
2	Baboon	8.5554	2.3292	0.8232	0.8664
3	House	8.5429	2.3500	0.8559	**0.8555**
4	Lena	8.5288	2.3229	0.8834	**0.8538**
5	Peppers	8.5323	2.4390	0.8889	**0.8568**
6	Seaport	8.5741	2.3209	0.8555	0.8599

Table 3.NPCR results of six image encryption algorithms for grayscale images

No.	Image	CMT-IEA [9]	LSMCL-IEA [11]	CS-IEA [5]	HF-IEA [7]	KSA-IEA [1]	GSVD-IEA

1	Sample-1	0.996011	0.992154	0.043255	0.995948	0.996038	0.995976
2	Sample-2	0.996034	0.992405	0.043255	0.996041	0.996017	**0.996137**
3	Sample-3	0.995967	0.992395	0.043255	0.996173	0.996049	0.996004
4	Sample-4	0.996110	0.992184	0.043255	0.995806	0.996162	0.995994
5	Sample-5	0.996213	0.992183	0.043255	0.996131	0.996051	**0.996278**
6	Sample-6	0.996043	0.992392	0.043255	0.996301	0.996188	0.995939
7	Sample-7	0.995183	0.992036	0.043255	0.995928	0.995874	**0.995990**
8	Sample-8	0.995838	0.992228	0.043255	0.995989	0.996169	**0.996231**
9	Sample-9	0.996206	0.992121	0.043255	0.996071	0.996213	0.995843
10	Sample-10	0.995985	0.992043	0.043255	0.995929	0.995918	**0.996065**
11	Sample-11	0.995993	0.992199	0.043255	0.996003	0.995996	**0.996034**
12	Sample-12	0.996233	0.992149	0.043255	0.996137	0.996018	0.995954
13	Sample-13	0.995940	0.992382	0.043255	0.995943	0.995903	**0.995991**
14	Sample-14	0.996002	0.992499	0.043255	0.995828	0.996008	**0.996034**
15	Sample-15	0.996178	0.992431	0.043255	0.996179	0.995993	0.995846
16	Sample-16	0.996055	0.992403	0.043255	0.996089	0.995916	**0.996176**
17	Sample-17	0.995934	0.992274	0.043255	0.996195	0.996132	**0.996223**
18	Sample-18	0.996102	0.992392	0.043255	0.996102	0.996105	**0.996167**
19	Sample-19	0.996262	0.992218	0.043255	0.995984	0.996139	0.996005
20	Sample-20	0.996085	0.992199	0.043255	0.995993	0.995928	**0.996117**

Table 4.UACI results of six image encryption algorithms for grayscale images

No.	Image	CMT-IEA [9]	LSMCL-IEA [11]	CS-IEA [5]	HF-IEA [7]	KSA-IEA [1]	GSVD-IEA
1	Sample-1	0.334839	0.334735	0.000170	0.334324	0.335248	0.334698
2	Sample-2	0.334649	0.333724	0.000170	0.334111	0.334439	**0.334894**
3	Sample-3	0.334683	0.334827	0.000170	0.334794	0.334649	0.334546
4	Sample-4	0.334638	0.334312	0.000170	0.334634	0.334748	**0.334993**
5	Sample-5	0.334267	0.334730	0.000170	0.334205	0.334683	**0.334803**
6	Sample-6	0.334184	0.334634	0.000170	0.334834	0.334037	0.334003
7	Sample-7	0.334535	0.334538	0.000170	0.334275	0.334053	**0.334644**
8	Sample-8	0.334037	0.334637	0.000170	0.334492	0.334374	**0.334763**
9	Sample-9	0.334904	0.334784	0.000170	0.334549	0.334273	**0.335310**
10	Sample-10	0.334735	0.335136	0.000170	0.334965	0.334729	0.334466
11	Sample-11	0.334279	0.334174	0.000170	0.334372	0.334312	**0.334488**
12	Sample-12	0.334825	0.334421	0.000170	0.334394	0.335374	0.334579
13	Sample-13	0.334526	0.333756	0.000170	0.334983	0.334295	**0.335000**
14	Sample-14	0.334846	0.334745	0.000170	0.335131	0.334804	0.334356
15	Sample-15	0.334934	0.334036	0.000170	0.335427	0.334781	0.334761
16	Sample-16	0.334054	0.334483	0.000170	0.334512	0.334261	**0.334654**
17	Sample-17	0.334322	0.333935	0.000170	0.334111	0.334314	**0.335181**
18	Sample-18	0.334793	0.334428	0.000170	0.335310	0.334213	0.334110
19	Sample-19	0.334128	0.334127	0.000170	0.334492	0.333825	**0.334343**
20	Sample-20	0.334629	0.334028	0.000170	0.334844	0.334719	**0.335427**

Tab**le 5.**NCPR and UACI encryption algorithms results of four image for colour image

No.	Image	LSMCL-IEA [11]		CS-IEA [5]		KSA-IEA [1]		GSVD-IEA	
		NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
1	Airplane	0.992163	0.334638	0.043054	0.000671	0.996137	0.334647	**0.996234**	0.334589

2	Baboon	0.992358	0.334974	0.043054	0.000677	0.996294	0.334934	0.996009	0.334897
3	House	0.992245	0.334922	0.043054	0.000337	0.995912	0.334783	**0.996061**	**0.334996**
4	Lena	0.992583	0.334493	0.043054	0.000337	0.996162	0.334734	0.996057	**0.334890**
5	Peppers	0.992499	0.334629	0.043054	0.000678	0.996152	0.334294	**0.996296**	**0.334677**
6	Seaport	0.992294	0.334693	0.043054	0.001347	0.996021	0.334535	**0.996198**	**0.334712**

Table 6. Correlation coefficients of six image encryption algorithms for sample-1 image

Direction	Plain-image	CMT-IEA [9]	LSMCL-IEA [11]	CS-IEA [5]	HF-IEA [7]	KSA-IEA [1]	GSVD-IEA
Horizontal	0.977898	0.002855	0.001954	0.001973	0.001869	0.001844	**0.001341**
Vertical	0.992487	0.002754	0.001349	0.002358	0.002347	0.002021	**0.002086**
Diagonal	0.973249	0.002644	0.002392	0.001736	0.001968	0.001759	**0.001323**

Table 7. Correlation coefficients of four image encryption algorithms for Lena image

Component	Direction	Plain image	LSMCL-IEA [11]	CS-IEA [5]	KSA-IEA [1]	GSVD-IEA
R	Horizontal	0.986389	0.001267	0.000693	0.001275	**0.000301**
	Vertical	0.953685	0.001473	0.001736	0.001864	**0.000989**
	Diagonal	0.986437	0.001699	0.002788	0.001853	**0.001282**
G	Horizontal	0.986462	0.001274	0.001526	0.001759	**0.000976**
	Vertical	0.977642	0.001228	0.001738	0.001533	**0.001058**
	Diagonal	0.966474	0.001479	0.001573	0.001635	**0.001387**
B	Horizontal	0.948970	0.001853	0.001019	0.001492	**0.000985**
	Vertical	0.936278	0.002856	0.002278	0.001724	**0.001374**
	Diagonal	0.936437	0.001643	0.001693	0.002189	**0.001388**

Table 8. Information entropy results of six image encryption algorithms for grayscale images

No.	Image	CMT-IEA [9]	LSMCL-IEA [11]	CS-IEA [5]	HF-IEA [7]	KSA-IEA [1]	GSVD-IEA
1	Sample-1	7.999323	7.999274	7.999329	7.999283	7.999310	**7.999342**
2	Sample-2	7.999247	7.999248	7.999214	7.999284	7.999314	**7.999329**
3	Sample-3	7.999311	7.999327	7.999295	7.999284	7.999330	**7.999341**
4	Sample-4	7.999339	7.999296	7.999275	7.999346	7.999386	7.999298
5	Sample-5	7.999284	7.999277	7.999267	7.999302	7.999303	**7.999311**
6	Sample-6	7.999209	7.999392	7.999434	7.999343	7.999326	7.999252
7	Sample-7	7.999299	7.999374	7.999246	7.999235	7.999383	7.999301
8	Sample-8	7.999137	7.999330	7.999373	7.999332	7.999348	**7.999431**
9	Sample-9	7.999289	7.999280	7.999194	7.999356	7.999229	**7.999340**
10	Sample-10	7.999301	7.999286	7.999238	7.999310	7.999237	**7.999319**

11	Sample-11	7.999447	7.999336	7.999338	7.999323	7.999341	7.999293
12	Sample-12	7.999197	7.999245	7.999226	7.999212	7.999254	**7.999299**
13	Sample-13	7.999338	7.999256	7.999387	7.999250	7.999374	7.999277
14	Sample-14	7.999183	7.999397	7.999351	7.999273	7.999366	7.999309
15	Sample-15	7.999347	7.999355	7.999334	7.999449	7.999453	**7.999477**
16	Sample-16	7.999299	7.999295	7.999316	7.999305	7.999292	**7.999342**
17	Sample-17	7.999394	7.999328	7.999298	7.999301	7.999295	**7.999492**
18	Sample-18	7.999382	7.999337	7.999333	7.999348	7.999265	**7.999408**
19	Sample-19	7.999383	7.999394	7.999342	7.999275	7.999279	7.999323
20	Sample-20	7.999311	7.999237	7.999337	7.999423	7.999458	7.999356

Table 9. Information entropy of four image encryption algorithms for colour image

No.	Image	LSMCL-IEA [11]	CS-IEA [5]	KSA-IEA [1]	GSVD-IEA
1	Airplane	7.999311	7.999314	7.999290	**7.999347**
2	Baboon	7.999268	7.999329	7.999393	7.999319
3	House	7.999329	7.999272	7.999275	**7.999372**
4	Lena	7.999303	7.999312	7.999386	7.999340
5	Peppers	7.999323	7.999331	7.999339	**7.999351**
6	Seaport	7.999284	7.999283	7.999267	**7.999329**

6050