INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

Image encryption predicated on segmented singular value decomposition using FrFT

Ashish Ranjan
ashishranjan.biku@gmail.com
Bansal Institute of Science and Technology, Bhopal, Madhya Pradesh

Krishna Kant Nayak
krishnakant1986@gmail.com
Bansal Institute of Science and Technology, Bhopal, Madhya Pradesh

ABSTRACT

The protection of the digital information and pictures has an integral function in defense as well as biomedical image handling applications. The formula which is usually to be utilized for the protection of data gives strength from any sort of incorrect supplies to the unwanted consumer. The idea of share matrix $S^{(k,n)}$ for the creation of shares has been investigated. These types of shares give a strength to the security or encryption of the confidential information and images. In this article, paper illustrates the utilization of share generation idea for encryption of the digital pictures in the SVD domain. The singular value of the SVD component functions as a good choice to create the shares of the picture. To bring the further improvement in the robustness, we apply Fractional Fourier Transform (FrFT). The sequence of the FrFT $(\alpha 1, \alpha 2)$ combined with the singular vectors (i.e., U and V) parts of the initial/base image functions similar to keys. Most of the state-of-the-art techniques are also studied combined with the suggested technique. A variety of quantitative parameters such as for example speed, number of pixels change rate (NPCR), unified average changing intensity (UACI), entropy, correlation coefficient, key sensitivity and mean square error (MSE) have been completely researched to examine the overall performance of the suggested technique. We find our suggested technique works more effectively or perhaps comparable sufficiently.

Keywords— *FrFT, Share matrix generation, Image Encryption, Sensitivity*

1. INTRODUCTION

In the modern age, images are most utilized communication method in the various areas including business, medical, military *etc*. The accelerated advancement of different communicating systems, we encounter with the large requirements to protect the transferred data as these pictures are transmitted through the unprotected network system. The protection of the digital images takes on a huge role in data evaluation. Individuals usually want to maintain their data protected from unauthorized users. Therefore, several encryption approaches is necessary by us that may save or hide important info of the images. However, saving sensitive info at one node provides loose effectiveness. This obviously suggests the number of nodes need to be enough that can prevent any physical harm to the info.

Secure graphic sharing is certainly an interesting research subject in multimedia systems. Its function is to encrypt a primary picture into n distinct shares. Its methods have been talked about to safeguard the key information of image. It offers a advantage over the regular security technique such that the suspicious users in no way obtain picture regardless if some understanding of the secret known to suspicious users.

The idea of sharing matrix were presented [5]. Threshold (T, N) scheme is utilized to divide the secret info in pieces, referred to as shares. [1] Suggested a matrix projection strategy with [5] approach. Afterwards, [3] talked about the principle of random grids in visual cryptography. Chaotic keys along with the lowered size shares has also been applied [4].

Above listed approach predicated on secret sharing strategies are extremely vulnerable to channel mistake. If a single pixel in share is influenced, it distorts T pixels in the reconstructed image, where T >>> 1. We suggest an incredibly innovative approach which will use just a few information of the picture to produce the shares of the picture. we use the concept of singular value decomposition (SVD).This redundancy pro- vides a lot more effectiveness as the significantly less quantity of pixels are affected. To fortify the proposed algorithm from unauthorized users, we make use of FrFT (Fractional Fourier transform).To demonstrate the suggested algorithm, we present the whole encryption method using two keys (α1, α2). The utilization of various part of the image i.e., U and V as keys is the significant contribution to security.

2. BASICS OF FRFT AND SVD

We will talk about the basic idea of Singular Value Decomposition and Fractional Fourier Transform (FrFT).

2.1 Fractional Fourier Transform (FrFT)

The Fractional Fourier Transform (FrFT) [10] of any two-dimensional signal $f(a, b)$ is written as follows.

$$F_{\beta1,\beta2}(f(a,b)(p,q)) = \left[\frac{1}{2\pi}\sqrt{(1-icot(\beta_1))(1-icot(\beta_2)}\right] \times \int exp\left[\frac{i(a^2+p^2)cot(\beta_1)}{2} - iapcsc(\beta_1)\right] \times exp\left[\frac{i(b^2+q^2)cot(\beta_2)}{2} - iapcsc(\beta_2)\right] f(a,b)dadb, \quad (1)$$

Where [β , β] can be understood in Fig. 1. The inverse of FrFT can be evaluated by the negative of its order [β_1, β_2].

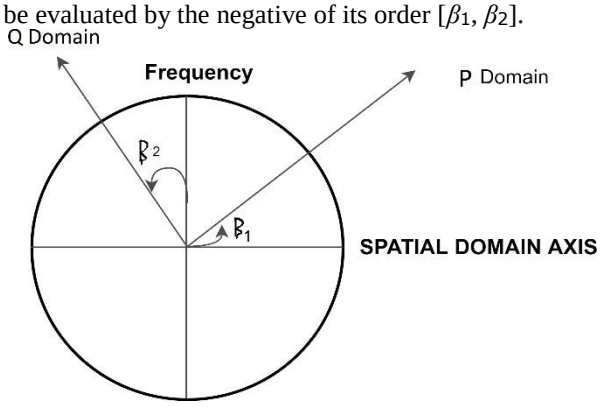

Fig. 1: FrFT in the p-q domain at an angle of β_1 and β_2. Here, β_1 and β_2 represent the order with respect to *a* and *b* axes respectively

Singular value decomposition (SVD): SVD work like mathematical device for the matrix analysis. It's a technique to get algebraic picture features or representations. The SVD matrix constructed for a digital image is highly stable. Singular value usually doesn't varies much with a minor transformation within an image. Any matrix A with p × q can be expressed as below.

$$A = U_a S_a V_a^T \quad (2)$$

Where, $U_a = [u_1^a, \dots, u_p^a] \in R^{p\times p}, V_a = [V_1^a, \dots, V_q^a] \in R^{q\times q}$ and $S_a = [diag\{u_1^a, \dots, u_p^a\}: 0] \in |R^{p\times q}$ is a diagonal matrix with p = minimum {|p,q|}.

Furthermore, more specifically, it can be given as below:

$$Y = \sum_{j=1}^{p} u_j^a \sigma_j^a v_j^{aT} \quad (3)$$

Idea of SVD has been put on several signal and image processing applications such as for example de-noising, image encryption [6] *etc.*

SVD: Singular values *S* are barely affected by noise or attacks *i.e.*,, if we observe the deterioration in image due to noise or attack, it hardly affects the singular values than singular vectors.

Therefore, impulsive tempering in singular vectors yields disastrous variations in the image quality [12]. Mathematically, we can present as follows.

$$K = [SM\{FrFT[S]\}] \quad (4)$$

Here, K as shares. Share matrix represented by SM which will be talked about in Section III.

3. PROPOSED ALGORTIHM

Let's discuss our recommended technique which includes two main actions.

- Generation of Share.
- Share Matrix Reconstruction

The method of encryption by FrFT is used for Share generation. α_1, α_2 are used respectively within the method. Primarily, the picture is normally divided in several parts applying SVD. Then after go with apply FrFT to the *S* matrix. Afterwards, paper [4] methods has been used to generate the shares of this matrix.

3.1 Sharing matrix - (k, n)

Assume $S_m^{(k,n)}$ be the binary matrix n×z that is, $S_m^{(k,n)}(j_1, j_2) \in [0,1]$ where the $1 \le j_1 \le n$ and $1 \le j_2 \le z$. Let say $A(r,j_2)$ be any p×z binary matrix, which is made by random choosing any p rows of $S_m^{(k,n)}$ with $1 \le p \le n$ and $1 \le r \le n$. $S^{(k,n)}$ must satisfy the conditions defined in equation 5 to equation 7.

- It should at least have one "1" in every row of $S_m^{(k,n)}$. We can represent it as follows.

$$\sum_{j_2=1}^{l} S_m^{(k,n)}(j_1, j_2) \neq 0 \quad (5)$$

- It must contain least one "1" in each column in the matrix A:

$$\sum_{r=1}^{p} A(r, j_2) \neq 0 \quad (6)$$

- Minimum one zero column in a matrix *A* when $p < k$,

$$\prod_{j_2=1}^{l}\left(\sum_{r=1}^{p} A(r, j_2)\right) = 0 \quad (7)$$

Where, $\sum_{r=1}^{p} A(r, j_2)$ provides addition with j_2^{th} column of matrix Z and $\prod_{j_2=1}^{l}(.)$ Is a successive multiplier function $S_m^{(k,n)}$ is called the (k,n)- sharing matrix. The fast algorithm for generation of $S^{(k,n)}$ has been discussed in [4]. The steps are as follow:

(a)Preliminary Matrix Generation: Initially a matrix A_1 having size of (2*k*-2) ×1 is constructed. A_1 is made up of (*k*-1) zeros and (*k*-1) ones. *E.g.*, A_1= [0 1 0 1 0 1]^T for k = 4. Afterwards, all of the possible permutations of A_1 are acquired, denoting A_y, y = 2,…,*N*, where $N = \frac{(2k-2)!}{(k-1)!(k-1)!}$. All these matrices needs to deliver the initial matrix S_0, shown in below formula (8).

$$S0 = [M_1, M_2, \dots, M_N] \quad (8)$$

(b) Matrix Expansion: Initially, matrix expansion is to ex- tent the matrix S_0 by appending extra 1. Expansion of matrix step's generate an increased matrix S_e. Paper [4] describes the more details.

3.2 Process of Sharing

Let's consider we get info matrix Q by following the encryption procedure over the picture by applying the FRFT. Table 1 shows the matrix. A share matrix $S_m^{(k,n)}$ with size n×l is presented in table 2. We opted real-valued matrix for elaboration. Although, FRFT gives an imaginary valued matrix. Thus, our proposed solution is also applied for the imaginary valued matrix. Every action for producing the shares have been talked about in Algorithm 1.

1	1	2	4	3	4
2	3	3	2	4	3
3	2	1	3	2	2
4	5	5	1	5	1
5	4	4	5	1	6
6	6	6	6	6	5

Table 1: Base data in a matrix of size=6 × 6

1	1	0	1	0	0
1	0	1	0	1	0
0	1	1	0	0	1
0	0	0	1	1	1

Table 2: Share matrix with k = 3 and n = 4

Algorithm 1: Share generation algorithm
1. Consider any gray-scale image 'Q' as shown in Table I.
2. For a constant value of n and k, produce share matrix $S^{(k,n)}$ as provided in Table II.
3. Translate Q into a vector Q.
4. Translate Q into Q1 such that $Q_1(j, :) = Q$, j = 1, . . . , n.
5. Do it again $S^{(k,n)}$to make it equal to Q_1.
6. Create shares Z such that $Z = Q_1 S_1$.
7. Every row of Z is called share.

3.3 Process of Reconstruction

This phase will prove that the matrix Q can be properly reconstructed only when the number of shares *i.e.*, $k_r \geq k$ are put together at the receiver end.

Below equation displays the whole procedure of joining k_r shares in between the recreation. Initially, a matrix R_m with a similar dimension of R is produced. R_m comprises of k_r rows of $1s$ and $0s$. Applying R_m, k_r rows of information from R are chosen to obtain R_1.

$$R1 = R * Rm = Q1 * S * Rm \quad (9)$$

In this way now the reproduction procedure creates a reconstructed matrix R_r

$$Rr(j) = R1(1,j)||R1(2,j)||,\ldots,||R1(n,j) = Q(j) * Rs(j),$$

(a) Reconstruction when $k_r = 3$ shares: In this article, we look the quantity of shares as 3. We generate R_m randomly which contains three '1' and one '0'. It is shown in equation 10 and equation 11.

$$R_m(3,1) = \begin{bmatrix} 1_{1\times 36} \\ 1_{1\times 36} \\ 1_{1\times 36} \\ 0_{1\times 36} \end{bmatrix}, \quad R_m(3,2) = \begin{bmatrix} 1_{1\times 36} \\ 1_{1\times 36} \\ 0_{1\times 36} \\ 1_{1\times 36} \end{bmatrix} \quad (10)$$

$$R_m(3,3) = \begin{bmatrix} 1_{1\times 36} \\ 0_{1\times 36} \\ 1_{1\times 36} \\ 0_{1\times 36} \end{bmatrix}, \quad R_m(3,4) = \begin{bmatrix} 0_{1\times 36} \\ 1_{1\times 36} \\ 1_{1\times 36} \\ 0_{1\times 36} \end{bmatrix} \quad (11)$$

Algorithm 2: Algorithm of Reconstruction
1. Apply FrFT (Fractional Fourier transform) with the order (β_1, β_2).
2. Gather the 3 shares i.e., any 3 rows of R.
3. The value of n and k_r, formulate $R_m(3, 1)$, $R_m(3, 2)$, $R_m(3, 3)$, and $R_m(3, 4)$ using mathematical 10 and Equation 11.
4. Multiply R with different Rm. Mark it as $R_1(3, 1)$, $R_1(3, 1)$, $R_1(3, 1)$, and $R_1(3, 1)$.
5. Afterwards, Using each R column-wise produces matrix $R_1^{(3,1)}, R_1^{(3,2)}, R_1^{(3,3)}$ *and* $R_1^{(3,4)}$
6. Each line comprises of the full picture
7. Besides, reshaping these row delivers the separated information/data matrix.

Algorithm 3: Proposed algorithm for share generation using fractional Fourier transform
1. Bring SVD of the grayscale image with dimension = 256× 256
2. Start the sequence for fractional Fourier transform *i.e.*, β_1 and β_2.
3. Initialize the (n, k) for our proposed method.
4. Determine the FrFT of matrix S with order β_1 and β_2. This generates the matrix of same size *i.e.*, 256×256.
5. Incorporate the idea of share matrix (SM) on the fractional order Fourier transform of the singular value matrix S.
6. For a constant value of n, k, and fractional Fourier of the image, we construct shares using Algorithm 1.
7. The measurement of the shares can be lowered. Nevertheless, we demonstrate our suggested method with the same dimension *i.e.*, 256×256.
8. At receiver end point, we initially decode k_r shares with the same k, n.
9. Finally, keeping the same order β_1 and β_2, the original image can be obtained. We shows with the minimum $k_r = 3$ shares. In the Fig. 3, we demonstrate the result as for changes in requests with $k_r = 2$ and $k_r = 3$.

Figure 2 depicts the suggested technique including the comprehensive algorithm. At first, the grayscale picture is broken into its constituents utilizing SVD. Share generation which is inredis the two major steps. Using S matrix, we create the shares of the image with method described in the paper [4]. The keys (β_1, β_2) hold an essential part in encryption. The other parts of the image U and V work as the keys. The bigger key space shows the robustness of the proposed algorithm.

4. OUTCOMES AND DISCUSSION

In this section, we analyze the quantitative parameters which are utilized for the similar investigation of the recommended strategy with various state-of-the-art methods.

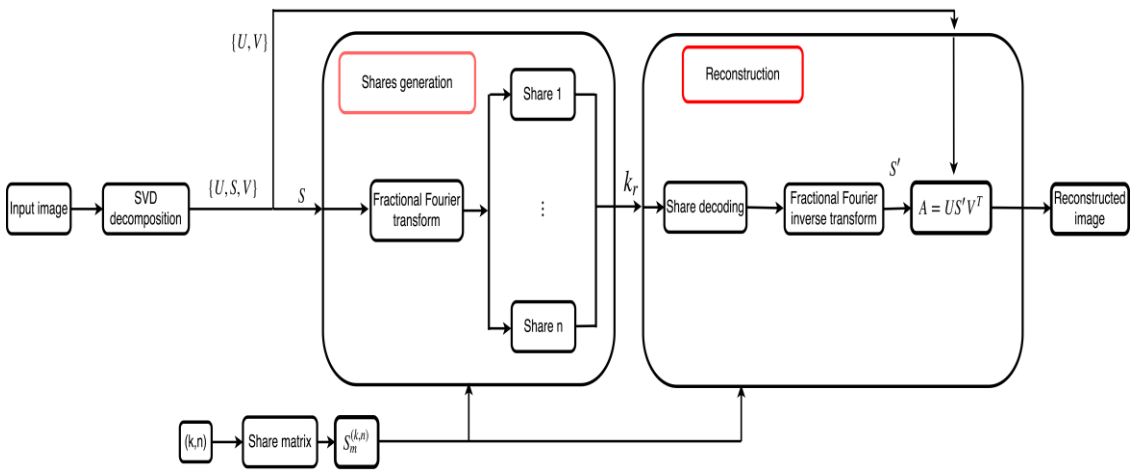

Fig. 2: The suggested technique including the comprehensive algorithm

4.1 Quantitative Parameters

(a) NPCR: Number of Pixels Change Rate: The number of pixels changes rate (NPCR) [7] displays the count of changed pixels when the power estimation of one pixel of the plain (or unique) picture is rotated. This speaks to the affectability of the proposed strategy to the adjustments in a single pixel. In this way, NPCR may make sense of the ability of a proposed technique against the harm on the plain picture.

$$NPCR = \frac{\sum_{m,n} X(m,n)}{W \times H} \times 100\ \% \qquad (12)$$

Where, where X(m, n) = 1, if $I_1(m, n) \neq I_2(m, n)$ (where I_1 and I_2 are the encrypted images for the given original image and the image which is one pixel different than the original image respectively), else D(m, n) is assumed as 0. H and W represent the height and width of the image respectively.

(b) UACI: Unified Average Changing Intensity: Unified average changing intensity (UACI) [7] display the mean intensity of variations among the related ciphered picture and the original picture. Hence, UACI can find out the ability of any such methods which can tolerate with the differential attacks.

$$UACI = \frac{1}{W \times H}\left[\sum_{mn} \frac{I_1(mn,) - I_2(m,n)}{255}\right] \times 100\% \quad (13)$$

Where I_1 is encrypted picture for the given baseline picture, I_2 is the encrypted picture related to the picture which is one pixel different than the baseline picture.

(c) SSIM: Structural Similarity Index Metric: In order to get the quality of the perceived image, SSIM is considered a unique parameter. Wang and Bovik [2] suggested SSIM and talked that it resides between -1 and 1. The mathematical representation can be provided as follows.

$$SSIM(a,b) = \frac{(2\mu_a\mu_b + c_a)(b\sigma_{ab} + c_b)}{(\mu_a^b + \mu_b^b + c_a)(\sigma_a^b + \sigma_b^b + c_b)} \qquad (15)$$

where μ_a, μ_b shows the mean value of picture a and picture b respectively. However, σ_a^b *and* σ_b^b displays the difference of the picture a and picture b respectively. σ_{ab} denotes the covariance between the image a and image b and c_a = 6.5025 and c_b = 58.5225 are predefined constants. Here, a represents the original picture and whereas b represents the encrypted picture

4.2 Quantitative Evaluation

In this section, we clarify the unique quantitative parameters for the evaluation which makes our solutions increasingly powerful. We tried our proposed technique on in excess of 20 diverse grayscale pictures. Be that as it may, we demonstrate the outcomes for cameraman picture

(a) Speed Efficiency: To show on the performance, all stud- ies are carried out on MATLAB 2016b with 8GB RAM and Intel(R) Core(TM)i3-4005U CPU @ 1.70 GHz. The picture encrypted by our proposed algorithm in 0.16425 sec.

(b) Differential Attacks: We utilized the impact of differential problems [7] to evaluate the suggested solution. We test NPCR and UACI. The mathematical formulas for NPCR and UACI have already been given in Equation (12) and Equation (13) respectively. The average value of NPCR for image is 95.98% at [β1 = 0.5, β2 = 0.2]. However, our proposed method produces UACI as 11.87%. This shows that our suggested solution is effective for any differential problems & attacks.

(c) IE: Information Entropy: IE demonstrates the haphazardness of the data. In a perfect world, it must be 8 so as to have consistency in the encoded pictures. Here, the data entropy of the scrambled pictures utilizing our proposed technique ≈1.8254. It is appeared Table 3. Nonetheless, outwardly the encoded pictures can be found in figure 3. In this manner, we can legitimize that our proposed strategy produces tasteful outcomes.

(d) Correlation Analysis: To ponder the similitude between two contiguous pixels of the scrambled picture, we inspect the idea of correlation. In the picture encryption method, the connection betweens two adjoining pixels ought to have low value. This ensures the scrambled picture can't be decoded without realizing the precise keys [7]. In Table IV, we show the correlation horizontally, vertically and diagonally. The lower value indicates that our encrypted picture with the suggested technique is nearly unachievable to decrypt without being aware of precise keys and its arrangements.

(e) Key Sensitivity: In this section, we learn the impact of a minor change in keys with which it must be decoded. A vigorous encryption procedure must have high affectability to- wards the mystery keys. We scrambled picture with β1 = 0.5, β2 = 0.2. When we unscramble the encoded picture with a slight change in keys i.e., β1 = 0.5000000000001, β2 = 0.2000000000001, we couldn't recover a careful reproduction of the first picture. It can be observed in Figure 3.

Table 3: NPCR, UACI, and Entropy of every shares of encrypted pictures.

Sr. no.	Picture	Shares	NPCR	UACI	Entropy
1.	'Img1'	Share1	95.98 %	11.87 %	1.8254
		Share2	95.98 %	11.87 %	1.8254
		Share3	95.98 %	11.87 %	1.8254
		Share4	95.98 %	11.87 %	1.8254

Table 4: Correlation coefficients of every shares of encrypted pictures

Sr. no.	Image	Shares	Horizontal	Vertical	Diagonal
1.	'Img1'	Share1	0.1532	0.0054	0.1804
		Share2	0.1532	−0.0322	−0.0124
		Share3	0.1532	0.0434	0.0767
		Share4	0.1532	0.3122	0.0767

Table 5: MSE (Mean Square Error) of every shares of encrypted pictures for various state-of-the-art methods. Take, p = e−10, t = e−15

Sr. no.	Image	Shares	Prop.	[9]	[11]	[4]	[8]
1.	'Img1'	Share1	0	2.001p	0	8.1304t	1.103t
		Share 2	0	2.001p	0	8.1304t	1.103t
		Share 3	0	2.001p	0	8.1304t	1.103t
		Share4	0	2.001p	0	8.1304t	1.103t

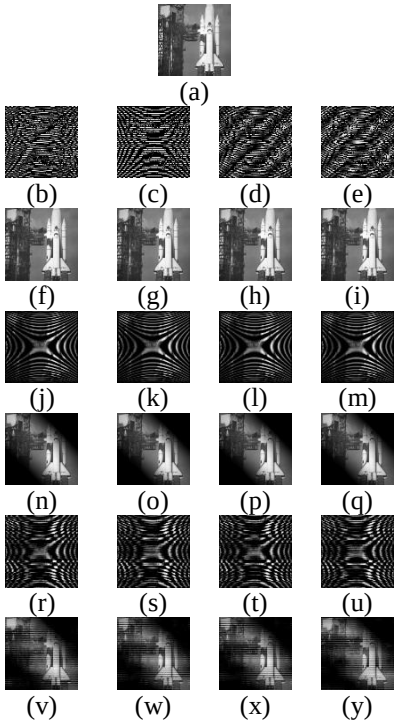

Fig. 3: (a) Original Satellite Rocket image (b)–(e) generated shares by suggested technique at fractional sequence (0.5,0.2) (f)–(i) reconstructed picture by suggested technique at fractional sequence (0.5,0.2) when k_r = 3; (j)–(m) reconstructed picture by suggested technique at fractional sequence (0.501,0.109) when k_r = 3; (n)–(q) reconstructed picture by suggested technique at fractional sequence (0.5000000000001,0.2000000000001) when k_r = 3; (r)–(u) reconstructed picture by suggested technique at fractional sequence (0.501,0.109) when k_r = 2; (v)–(y) reconstructed picture by suggested technique at fractional sequence (0.5000000000001,0.2000000000001) when k_r = 2.

4.3 Comparison to state-of-the-art techniques

In this section, we contrast our outcomes and some state- of-the-art techniques, for example, [9], [11], [4], and [8] in terms of quantitative parameter MSE between the base and the resulted pictures. Our SVD based suggested technique shows the exact same output. The MSE ('0') implies in Table V. It is obtained at the same key $\beta_1 = 0.5$, $\beta_2 = 0.2$.Moreover, different systems produce just about zero MSE. It demonstrates that our proposed method is practically equivalent to some notable state-of-the-art strategies.

5. CONCLUSION

In this paper, we initially portray the necessity of a hearty sharing strategy which can improve the security of the private information, for example, pictures, video *etc*. We discuss the formulations of sharing matrix -(k, n). The singular value matrix of the SVD decomposition is much more effective to any changing *i.e.*, noise or attacks.

After that, FrFT makes our proposed technique progressively powerful. The adjustments in the sequence of α_1, α_2 in the range 10^{-14} can't deliver the equivalent unscrambled picture. The MSE value as "0" simply shows that our suggested technique quite robust. Our future work incorporates the unscrambling of various attacks and superior processing, adaptable and solid registering equipment structure execution on field programmable gate array.

6. REFERENCES

[1] L Bai, "A reliable (k, n) image secret sharing scheme with low information overhead," *Int. Journal of Compt. Appl.*, vol. 32, no. 1, pp. 9–14, 2010.

[2] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Trans. Image*, vol. 13, pp. 600–612, 2004.

[3] R. Wang, Y. Lan, Y. Lee, S. Y. Huange, S. Shyu, and T. L. Chia, "Incrementing visual cryptography using random grids," *Opt. Commn.*, vol. 283, no. 21, pp. 4242–4249, 2010.

[4] L. Bao, S. Yi, and Y. Zhou, "Combination of Sharing Matrix and Image Encryption for Lossless (k, n) -Secret Image Sharing," *IEEE Transactions on Image Processing*, vol. 26, no. 12, pp. 5618–5631, 2017.

[5] A.Shamir, "How to share a secret," *Communication of ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[6] O. Alter, P. O. Brown, D. Botstein, "Singular value decomposition for genome-wide expression data processing and modeling," *PNAS*, vol. 97, no. 18, pp. 10101–10106, 2000.

[7] H. S. Kwok, and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos Solitons Fractals*, vol. 32, pp. 1518–1529, 2007.

[8] S. Wang, "Distributed Storage scheme Based on Secret Sharing Schemes" School of Electrical and Computer Engineering, University of Oklahoma, Tulsa, OK, USA.

[9] C. N. Yang, and D. S. Wang, "Property analysis of XOR-based visual cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 2, pp. 189–197, 2014.

[10] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, "The Fractional Fourier Transform with applications in optics and signal processing," *Wiley*, pp. 1–75, 2001.

[11] X. Wu, and W. Sun. "Extended capabilities for XOR-based visual cryptography," *IEEE Trans. Inf. Forensic Security*, vol. 9, no. 10, pp. 1592–1605, 2014.

[12] K. Konstantinides, B. Natarajan, and G.S. Yovanof, "Noise estimation and filtering using block-based singular value decomposition," *IEEE Trans. Image Processing*, vol. 6, no. 3, pp. 479–483, 1997.

