Journal of Theoretical and Applied Information Technology
15th July 2018. Vol.96. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

KEY LOGISTIC TO IMAGE CRYPTOGRAPHY VIA GENERAL SINGULAR VALUES DECOMPOSITION

[1]MAHER JALAL BURJUS AL-BASHKANI , [2]PROF. DR. ADIL AL- RAMMAHI

[1]Department of Mathematics, faculty of computer science and mathematics, University of Kufa, Al-Najaf, Iraq

[2]Department of Mathematics, faculty of computer science and mathematics, University of Kufa, Al-Najaf, Iraq

E-mail : [1] maherj.albashkani@student.uokufa.edu.iq , [2] adilm.hasan@uokufa.edu.iq

ABSTRACT

Cryptography is one of the most important topics of this era after the introduction of technology into most aspects of life. It was necessary to protect the property of private documents and important files, which we use in its understandable form such as texts, pictures, sounds, folders and other information .

The purpose of image cryptography is to maintain the security and confidentiality of information against the process of breaking the image code , as it is a coding application where it encrypts the images want we to keep from tampering with the intruders.

This paper deals with the method of general singular value decomposition algorithm with logistic function . To strengthen our algorithm, a key was used during a general singular value decomposition algorithm. First , We generated a key and then used it to encode the selected image via general singular value decomposition algorithm.

For testing the powerful of proposed algorithms, many recent related algorithms were studied and compared. All programs had been executed by the MATLAB. The results were very encouraged.

Keywords : *Image Cryptography Via General Singular Values Decomposition With Logistic Function*

1. INTRODUCTION

Cryptography is the process of preserving the confidentiality of information by using math algorithms that have the ability to translate that information into unknown symbols so that if the strangers people who are not authorized to do so. Then they are not understand anything because what appears to them is a combination of symbols, numbers and unintelligible letters [1] [2] .

Therefore, the word "encrypt" refers to the conversion or "bumping" of data into an incomprehensible entity to be sent through a particular vector to a specific destination. So that no party other than the intended destination can interpret this data and extract the data that is understood from it and this process is the highest possible safety .

This paper proposes a new algorithm in which variables are treated as cryptographic codes in order to achieve safe transfer of color digital images .In this algorithm the data is encrypted during general singular value decomposition algorithm. For improving the powerful of proposed algorithm against cryptanalysis we used the chaotic logistic function as a key. Then the digital plain image was encrypted via general singular value decomposition algorithm.

2. LOGISTIC FUNCTION

The basic information of map Logistic and its modifications is presented in this section. The behaviors of four types of one dimensional Logistic function are gathered in a table via our programmed of displaying graphs [3] .

2.1 Logistic Map

Logistic Map is map one-dimensional which is used to systems model simple nonlinear and

Journal of Theoretical and Applied Information Technology
15th July 2018. Vol.96. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

discrete . Logistic map is explained by a function recursive as follows :

$$x_{n+1} = L(r.x_n) = r * x_n * (1 - x_n) \dots \dots \dots (1)$$

where r is parameter and $x_n \in [0.1]$. Consider Logistic Map
$L : [0.1] \rightarrow [0.1]$, by given Equation (1), the pa−rameter r lies in interval [0.4] . The map return of given Logistic function in for $r = 4$.

There is sensitivity suitable to initial condition. In order to view the chaotic properties of Logistic Map , exponent Lyapunov and bifurcation and diagram of it should be plotted and calculated . The diagram of Bifurcation of map with Logistic respect to "r" are plotted and calculated.

2.2. Modified Logistic Maps

Exponent Lyapunov of Logistic Map with respect to "r" are plotted and calculated . Logistic Map is chaotic when parameter "r" lies in interval [3.6. 4] [3].

For the process could be defined as depicted in Equation (2), such that $g(x)$ and $h(x)$are the left and right hand side functions, respectively

$$x_{n+1} = f(x_n) = \begin{cases} g(x_n) \, . x_n < a \\ h(x_n) \, .. x_n \geq a \end{cases} \dots \dots \dots \dots (2)$$

where $x_n \in [0.1]$ and $a \in (0.1)$
The necessary condition for a two segmental function $f = \{g.h\}$ to be a Lebesgue process is that the absolute value of slops must be greater than unity all over the domain. That is, the absolute of derivatives of two
branches over the range must be greater than one according to equation (3) .

$$|f'(x)| > 1 \text{ for} : x \in [0.1] \dots \dots \dots \dots (3)$$

As far as Logistic map is concerned, its equation could be separated as follows with respect to $a = 0.5$

$$x_{n+1} = L(r.x_n) = \begin{cases} g(x_n) = r \cdot x_n \cdot (1 - x_n) \, . & x_n < a \, ; \\ h(x_n) = r \cdot x_n \cdot (1 - x_n) \, . & x_n \geq a \, ; \end{cases} \dots \dots (4)$$

Considering Equation (4), the derivatives of $g(x)$ are exceeding unity, but this is not true for $h(x)$. To solve this problem, we use symmetry and transform properties to modify $h(x)$. Actually, we modified the second part of Logistic map in order to improve the chaotic range of Logistic map in two manners [3] .

2.3 Types of Logistic Functions through the Effect of K Value on them and According to the Program we Prepared

For calculating the points logistic function in R^2 , where
f(x)=kx(1-x), K>0, 0≤x≤1,

one can classified the logistic functions into four types with respect to the sensivity of the value of k, and as follows in TABLE 1 and 2,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1 : The Types Of Logistic Function

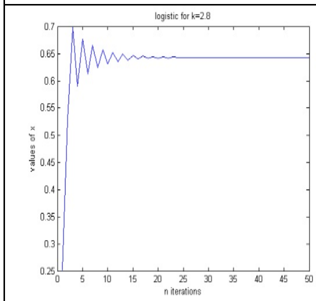
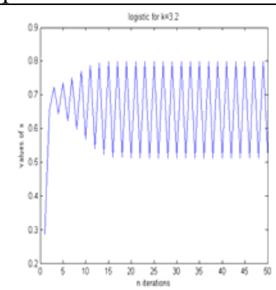
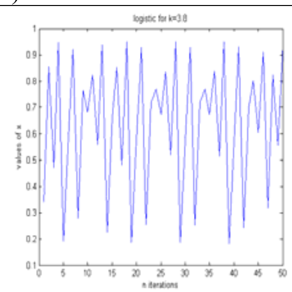
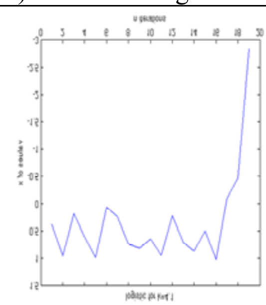
1) k=2.8: Stable 1-point	2) K=3.2: Stable 2-cycle point
	
3) K=3.8: Chaotic	4) K=4.1: Divergent
	

Table 2 : The Behavior Of Logistic Function

No	Dynamical Behavior	Value of k
1	Stable Point	0<k<2
2	Stable m-Point Cycle	2<k<3.5
3	Chaos	3.5<k<4
4	Unstable	k>4

3. GENERALIZED SINGULAR VALUE DECOMPOSITION :

For a given $I \times J$ matrix A, generalizing the singular value decom-position, involves using two positive definite square matrices with size $I \times J$ and $J \times J$ respectively. These two matrices express con-straints imposed respectively on the rows and the columns of A. Formally, if M is the $I \times I$ matrix expressing the constraints for the rows of A and W the $J \times J$ matrix of the constraints for the columns of A. Matrix A is now decomposed into [4] :

$$A = \tilde{U}\tilde{\Delta}\tilde{V}^{T} \quad \text{with} : \tilde{U}^{T}M\tilde{U} = \tilde{V}^{T}W\tilde{V} = I \qquad (5)$$

In other words, the generalized singular vectors are orthogonal under the constraints imposed by M and W.

This decomposition is obtained as a result of the standard singular value decomposition. We begin by defining the matrix $\tilde{A}$ as:

$$\tilde{A} = M^{\frac{1}{2}}AW^{\frac{1}{2}} \Leftrightarrow A = M^{-\frac{1}{2}}\tilde{A}W^{-\frac{1}{2}} \qquad (6)$$

We then compute the standard singular value decomposition as:

$$\tilde{A} = P\Delta Q^T \quad \text{with}: \; P^TP = Q^TQ = I \qquad (7)$$

The matrices of the generalized eigenvectors are obtained as:

$$\tilde{U} = M^{-\frac{1}{2}}P \quad \text{and} \quad \tilde{V} = W^{-\frac{1}{2}}Q \qquad (8)$$

The diagonal matrix of singular values is simply equal to the matrix of singular values of $\tilde{A}$:

$$\tilde{\Delta} = \Delta \qquad (9)$$

We verify that:

$$A = \tilde{U}\tilde{\Delta}\tilde{V}^T$$

by substitution:

$$A = M^{-\frac{1}{2}}\tilde{A}W^{-\frac{1}{2}}$$
$$A = M^{-\frac{1}{2}}P\Delta Q^TW^{-\frac{1}{2}}$$

$$A = \tilde{U}\Delta\tilde{V}^T \text{ (from Equation 8)} \qquad (10)$$

from Equation 5 , suffice to show that:

$$\tilde{U}^TM\tilde{U} = P^TM^{\frac{1}{2}}MM^{-\frac{1}{2}}P = P^TP = I \qquad (11)$$

And

$$\tilde{V}^TW\tilde{V} = Q^TW^{-\frac{1}{2}}WW^{-\frac{1}{2}}Q = Q^TQ = I \qquad (12)$$

It is in several types It enters into a lot of applications, within the matrices algebra field in particular, and in general applied mathematics. In this paper, we are satisfied with clarifying it to the dear reader and making it simple, until it is clear to him\her the role of this analysis in encryption [6][12][14].

Singular Value Generalized Decomposition(GSVD).

$[U.V.X.C.S] = GSVD(A.B)$ returns unitary matrices U and V, square matrix X , and diagonal matrices nonnegative C and S so that

$$A = U * C * X^T$$

$$B = V * S * X^T$$

$$C^T * C + S^T * S = I$$

A and B the columns in the two must be equal, but may have different numbers of rows. If A is $m-by-p$ and B is $n-by-p$, then U is $m-by-m$, V is $n-by-n$ and X is $p-by-q$ where $q = \min(m+n.p)$.

$SIGMA = GSVD(A, B)$ returns the direction of singular values generalized, $\text{sqrt}(\text{diag}(C^T * C)./\text{diag}(S^T * S))$.

The nonzero elements of S are usually on its diagonal main . If $m >= p$ the nonzero elements of C are also on its diagonal main. But if $m < p$, the nonzero diagonal of C is $\text{diag}(C.p-m)$. This allows the diagonal elements to be ordered so that the singular values generalized are non-decreasing. $GSVD(A, B, 0)$, with input arguments three and either m or $n >= p$, produces the "economy-sized" the resulting where decomposition U and V have at most p columns, and C and S have at most p rows.

The general singular values are $\text{diag}(C)./\text{diag}(S)$. When $I = \text{eye}(\text{size}(A))$, the general singular values , $\text{gsvd}(A.I)$, are to equal the singular values ordinary, $\text{svd}(A)$,but in the opposite order they are sorted . Their reciprocals are $\text{gsvd}(I, A)$.

In GSVD format, assumptionswillbe made about the individual ranks of A or B. The matrix X has full rank if and only if the matrix [A; B] has full rank. In fact, svd(X) and cond(X) are equal to svd([A; B]) and cond([A; B]). Other formulations, eg.

G. Golub and C. Van Loan, " Computations Matrix ", that require null(A) and null(B) do not replace and overlap X by inv(X) or inv(X^T)

Note, that when , however, null(A) and null(B) do overlap, the nonzero elements of C and S are not determined uniquely.

An example of a GSVD method is using the MATLAB program

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix} \text{ and } B = \begin{bmatrix} 7 & 8 \\ 9 & 1 \end{bmatrix}$$

$[U.V.X.C.S] = \text{gsvd}(A.B)$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$U = \begin{bmatrix} 0.8679 & -0.2830 & 0.4082 \\ 0.2085 & -0.5384 & -0.8165 \\ -0.4508 & -0.7938 & 0.4082 \end{bmatrix}$$

$$V = \begin{bmatrix} -0.0881 & -0.9961 \\ -0.9961 & 0.0881 \end{bmatrix}$$

$$X = \begin{bmatrix} -9.6121 & -8.5211 \\ -1.7065 & -10.8668 \end{bmatrix}$$

$$C = \begin{bmatrix} 0.0791 & 0 \\ 0 & 0.6885 \\ 0 & 0 \end{bmatrix}$$

$$S = \begin{bmatrix} 0.9969 & 0 \\ 0 & 0.7252 \end{bmatrix}$$

4. PROPOSED ALGORITHM

The proposed algorithm is for encrypting and decoding images where the logistic function and GSVD method were used. The proposed algorithm will include narrowing of the image using the logistic function together with the k key. We will get two matrices, one multiplied by k and the other by $-k$, and then using GSVD with one of the two resulting array of the logistic function and the gsvd method, which is a GSVD and the image encryption and thus an encrypted image will be obtained .

When we decryption happens , the encrypted image is identified and the gsvd method is used and the image used as a key in the gsvd format, the image is analyzed. This is done by part of the image decoding and then the logistic function is used to decode the image. This will be done by decoding the image and getting the original image .

The Encryption Part

1. Start with virtual dimensions rather than with mandatory dimensions and the algorithm is applied for any image and in any dimensions .
2. Input an image of any size ; in this case, 512 × 512 (this algorithm is applied for any image and in any dimension) .
3. Convert the image to a matrix A_1 .
4. Choose a key to use as a key with a logistic function and an account :
$$A_2 = k. * A_1 * (255 - A_1)$$
$$AA_1 = k. * A_2$$
$$AA_2 = -k. * A_2$$
5. Choose an encrypting key image that can be converted to a matrix B .
6. Compute the GSVD for each matrix AA_1 and AA_2 with the encrypt ing key matrix B as follows :
$$\begin{cases} [u_1.v_1.x_1.c_1.s_1] = \text{gsvd}(AA_1.B) \\ [u_2.v_2.x_2.c_2.s_2] = \text{gsvd}(AA_2.B) \end{cases}$$
7. Compute the following :
$$\begin{cases} AAA_1 = u_1 * c_2 * x_1^t \\ AAA_2 = u_2 * c_1 * x_2^t \end{cases}$$
8. Construct the encrypted matrix as F such that ,
$$F = \begin{bmatrix} AAA1 \\ AAA2 \end{bmatrix}$$
9. The encrypted image Obtained is F .
10. End .

The Decryption Part

1. Start .
2. Download the encrypted image .
3. Obtain the matrix of the encrypted image which is called F .
4. Split F into AAA_1 and AAA_2 .
5. Obtain the decrypted key matrixB which is the same encrypted key matrix .
6. Obtain the decrypted key K which is the same encrypted key .
7. Compute the GSVD for each matrix AAA_1 and AAA_2 with the decrypting key matrix B follows :
$$\begin{cases} [uu_1.vv_1.xx_1.cc_1.ss_1] = \text{gsvd}(AAA_1.B) \\ [uu_2.vv_2.xx_2.cc_2.ss_2] = \text{gsvd}(AAA_2.B) \end{cases}$$
8. Compute the plain matrix A_{11} and A_{22} follows :
$$A_{11} = uu_1 * cc_2 * cx_1^t$$
$$A_{22} = uu_2 * cc_1 * xx_2{}^t$$
9. Compute the plain matrix A_1 follows:
$A_1 = \frac{A_{11}}{K}$Then use the following equation :
$$A_1{}^2 - 255A_1 - \frac{A_2}{K} = 0$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

one can get the matrix A_1

10. Got the original image
11. End

for test the proposed Algorithm , the following example is studied :

The Encryption Part :

1. Choose any image whatever its dimensions .
2. In this example we will choose a picture with dimensions $3 * 3$ (for example) .
3. convert the image to a matrix

$$A_1 = \begin{bmatrix} 2 & 4 & 130 \\ 5 & 6 & 9 \\ 180 & 1 & 100 \end{bmatrix}$$

4. Choose a key $K = 7$ to use as a key with a logistic function and an account :
$A_2 = k. * A_1 * (255 - A_1)$

$$A_2 = \begin{bmatrix} 3542 & 7028 & 113750 \\ 8750 & 10458 & 15498 \\ 94500 & 1778 & 108500 \end{bmatrix}$$

$$AA_1 = k. * A_2$$

$$AA_1 = \begin{bmatrix} 24795 & 49196 & 796250 \\ 61250 & 73206 & 108486 \\ 661500 & 12446 & 759500 \end{bmatrix}$$

$$AA_2 = -k. * A_2$$

$$AA_1 = \begin{bmatrix} -24795 & -49196 & -796250 \\ -61250 & -73206 & -108486 \\ -661500 & -12446 & -759500 \end{bmatrix}$$

5. Choose an encrypting key image that can be conv erted to a matrix

$$B = \begin{bmatrix} 170 & 7 & 10 \\ 1 & 155 & 2 \\ 8 & 100 & 5 \end{bmatrix}.$$

6. Compute the GSVD for each matrix AA_1 and AA_2 with the encrypt ing key matrix B follows :

$$[U_1 . V_1 . X_1 . C_1 . S_1] = gsvd(AA_1 . B)$$

$$U_1 = \begin{bmatrix} 0.0576 & -0.6735 & 0.7370 \\ -0.9952 & 0.0199 & 0.0959 \\ 0.0792 & 0.7389 & 0.6691 \end{bmatrix}$$

$$V_1 = \begin{bmatrix} -0.0814 & 0.9963 & -0.0294 \\ -0.8372 & -0.0843 & -0.5404 \\ -0.5408 & -0.0194 & 0.8409 \end{bmatrix}$$

$$X_1 = 10^6 * \begin{bmatrix} -0.0071 & 0.4733 & 0.4667 \\ -0.0690 & -0.0225 & 0.0516 \\ -0.0019 & 0.0271 & 1.1054 \end{bmatrix}$$

$$C_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 0.0027 & 0 & 0 \\ 0 & 0.0004 & 0 \\ 0 & 0 & 10 \end{bmatrix}$$

$$[U_2 . V_2 . X_2 . C_2 . S_2] = gsvd(AA_2 . B)$$

$$U_2 = \begin{bmatrix} -0.0576 & 0.6735 & -0.7370 \\ 0.9952 & -0.0199 & -0.0959 \\ -0.0792 & -0.7389 & -0.6691 \end{bmatrix}$$

$$V_2 = \begin{bmatrix} -0.0814 & 0.9963 & -0.0294 \\ -0.8372 & -0.0843 & -0.5404 \\ -0.5408 & -0.0194 & 0.8409 \end{bmatrix}$$

$$X_2 = 10^6 * \begin{bmatrix} -0.0071 & 0.4733 & 0.4667 \\ -0.0690 & -0.0225 & 0.0516 \\ -0.0019 & 0.0271 & 1.1054 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$S_2 = \begin{bmatrix} 0.0027 & 0 & 0 \\ 0 & 0.0004 & 0 \\ 0 & 0 & 10 \end{bmatrix}$$

7. Compute the following :

$$AAA_1 = U_1 * C_2 * {X_1}^T$$

$$AAA_1 = 10^5 * \begin{bmatrix} 0.2479 & 0.4920 & 7.9625 \\ 0.6125 & 0.7321 & 1.0849 \\ 6.6150 & 0.1245 & 7.5950 \end{bmatrix}$$

$$AAA_2 = U_2 * C_1 * {X_2}^T$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$AAA_2 = 10^5 * \begin{bmatrix} -0.2479 & -0.4920 & -7.9625 \\ -0.6125 & -0.7321 & -1.0849 \\ -6.6150 & -0.1245 & -7.5950 \end{bmatrix}$$

8. Construct the encrypted matrix as F such that ,

$$F = [AAA_1; AAA_2]$$

$$F = \begin{bmatrix} 0.2479 & 0.4920 & 7.9625 \\ 0.6125 & 0.7321 & 1.0849 \\ 6.6150 & 0.1245 & 7.5950 \\ -0.2479 & -0.4920 & -7.9625 \\ -0.6125 & -0.7321 & -1.0849 \\ -6.6150 & -0.1245 & -7.5950 \end{bmatrix}$$

9. Obtain the encrypted image F .

10. End the image encryption .

The decryption part :

1. Start decryption .

2. Download the encrypted image .

3. Obtain the matrix of the encrypted image, which is called F .

$$F = \begin{bmatrix} 0.2479 & 0.4920 & 7.9625 \\ 0.6125 & 0.7321 & 1.0849 \\ 6.6150 & 0.1245 & 7.5950 \\ -0.2479 & -0.4920 & -7.9625 \\ -0.6125 & -0.7321 & -1.0849 \\ -6.6150 & -0.1245 & -7.5950 \end{bmatrix}$$

4. Split F into AAA_1 and AAA_2 follows :

$$AAA_1 = F([1{:}end/2] .{:})$$

$$AAA_1 = 10^5 * \begin{bmatrix} 0.2479 & 0.4920 & 7.9625 \\ 0.6125 & 0.7321 & 1.0849 \\ 6.6150 & 0.1245 & 7.5950 \end{bmatrix}$$

$$AAA_2 = AAA([end/2 + 1{:}end] .{:})$$

$$AAA_2 = 10^5 * \begin{bmatrix} -0.2479 & -0.4920 & -7.9625 \\ -0.6125 & -0.7321 & -1.0849 \\ -6.6150 & -0.1245 & -7.5950 \end{bmatrix}$$

5. Obtain the decrypted key matrix

$$B = \begin{bmatrix} 170 & 7 & 10 \\ 1 & 155 & 2 \\ 8 & 100 & 5 \end{bmatrix}$$

which is the same encrypted key matrix .

6. Obtain the decrypted key K = 7 which is the same encrypted key .

7. Compute the GSVD for each matrix AAA_1 and AAA_2 with the decrypting key matrix B follows :

$$[UU_1 . VV_1 . XX_1 . CC_1 . SS_1] = gsvd(W_1 . B)$$

$$UU_1 = \begin{bmatrix} 0.0576 & -0.6735 & 0.7370 \\ -0.9952 & 0.0199 & 0.0959 \\ 0.0792 & 0.7389 & 0.6691 \end{bmatrix}$$

$$VV_1 = \begin{bmatrix} -0.0814 & 0.9963 & -0.0294 \\ -0.8372 & -0.0843 & -0.5404 \\ -0.5408 & -0.0194 & 0.8409 \end{bmatrix}$$

$$XX_1 = 10^6 * \begin{bmatrix} -0.0071 & 0.4733 & 0.4667 \\ -0.0690 & -0.0225 & 0.0516 \\ -0.0019 & 0.0271 & 1.1054 \end{bmatrix}$$

$$CC_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$SS_1 = \begin{bmatrix} 0.0027 & 0 & 0 \\ 0 & 0.0004 & 0 \\ 0 & 0 & 10 \end{bmatrix}$$

$$[UU_2 . VV_2 . XX_2 . CC_2 . SS_2] = gsvd(W_2 . B)$$

$$UU_2 = \begin{bmatrix} -0.0576 & 0.6735 & -0.7370 \\ 0.9952 & -0.0199 & -0.0959 \\ -0.0792 & -0.7389 & -0.6691 \end{bmatrix}$$

$$VV_2 = \begin{bmatrix} -0.0814 & 0.9963 & -0.0294 \\ -0.8372 & -0.0843 & -0.5404 \\ -0.5408 & -0.0194 & 0.8409 \end{bmatrix}$$

$$XX_2 = 10^6 * \begin{bmatrix} -0.0071 & 0.4733 & 0.4667 \\ -0.0690 & -0.0225 & 0.0516 \\ -0.0019 & 0.0271 & 1.1054 \end{bmatrix}$$

$$CC_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$SS_2 = \begin{bmatrix} 0.0027 & 0 & 0 \\ 0 & 0.0004 & 0 \\ 0 & 0 & 10 \end{bmatrix}$$

8. Compute the plain matrix A_{11} and A_{22} follows :

$$A_{11} = UU_1 * CC_2 * {XX_1}^T$$

$$A_{11} = 10^5 * \begin{bmatrix} 0.2479 & 0.4920 & 7.9625 \\ 0.6125 & 0.7321 & 1.0849 \\ 6.6150 & 0.1245 & 7.5950 \end{bmatrix}$$

$$A_{22} = UU_2 * CC_1 * {XX_2}^T$$

$$A_{22} = 10^5 * \begin{bmatrix} -0.2479 & -0.4920 & -7.9625 \\ -0.6125 & -0.7321 & -1.0849 \\ -6.6150 & -0.1245 & -7.5950 \end{bmatrix}$$

9. Compute the plain matrix A_1 follows :

$$A_1 = A_{11}/K$$

$$A_1 = 10^5 * \begin{bmatrix} 0.0354 & 0.0703 & 1.1375 \\ 0.0875 & 0.1046 & 0.1550 \\ 0.9450 & 0.0178 & 01.0850 \end{bmatrix}$$

Note

$$A_2 = K * A_1 * (255 - A_1)$$

$$\Longrightarrow A_2 = K * A_1 * (255 - A_1)$$

$$\Longrightarrow {A_1}^2 - 255A_1 - \frac{A_2}{K} = 0$$

We get the solution by experiment .

9.1. Root1 represents the element in row-1 and column-1

$Y = [\,1 - 255 \;\; A_1(1,1)/K\,]$
$Y = [\,1 \; -255 \;\; 506\,]$
$r_1 = \text{roots}(Y)$
$r_1 = 253$ or $r_1 = 2$

9.2. Root2 represents the element in row-1 and column-2

$Y = [\,1 - 255 \;\; A1(1,2)/K\,]$
$Y = [\,1 \; -255 \;\; 1004\,]$
$r_2 = \text{roots}(Y)$
$r_2 = 251$ or $r_2 = 4$

9.3. Root3 represents the element in row-1 and column-3

$Y = [\,1 - 255 \;\; A1(1,3)/K\,]$
$Y = [\,1 \; -255 \;\; 16250\,]$
$r_3 = \text{roots}(Y)$
$r_3 = 130$ or $r_3 = 125$

9.4.Root4 represents the element in row-2 and column-1

$Y = [\,1 - 255 \;\; A1(2,1)/K\,]$
$Y = [\,1 \; -255 \;\; 1250\,]$
$r_4 = \text{roots}(Y)$
$r_4 = 250$ or $r_4 = 5$

9.5.Root5 represents the element in row-2 and column-2

$Y = [\,1 - 255 \;\; A1(2,2)/K\,]$
$Y = [\,1 \; -255 \;\; 1494\,]$
$r_5 = \text{roots}(Y)$
$r_5 = 249$ or $r_5 = 6$

9.6.Root6 represents the element in row-2 and column-3

$Y = [\,1 - 255 \;\; A1(2,3)/K\,]$
$Y = [\,1 \; -255 \;\; 2214\,]$
$r_6 = \text{roots}(Y)$
$r_6 = 246$ or $r_6 = 9$

9.7.Root7 represents the element in row-3 and column-1

$Y = [\,1 - 255 \;\; A1(3.1)/K\,]$
$Y = [\,1 \; -255 \;\; 13500\,]$
$r_7 = \text{roots}(Y)$
$r_7 = 180$ or $r_7 = 75$

9.8.Root8 represents the element in row-3 and column-2

$Y = [\,1 - 255 \;\; A1(3,2)/K\,]$
$Y = [\,1 \; -255 \;\; 254\,]$
$r_8 = \text{roots}(Y)$
$r_8 = 254$ or $r_8 = 1$

9.9.Root9 represents the element in row-3 and column-3

$Y = [\,1 - 255 \;\; A1(3,3)/K\,]$
$Y = [\,1 \; -255 \;\; 15500\,]$
$r_9 = \text{roots}(Y)$
$r_9 = 155$ or $r_9 = 100$

Where each root represents an element in the array

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The color values of the correct A_1 matrix is specified and when decoding finishes original matrix is obtained .

$$A_1 = \begin{bmatrix} 2 & 4 & 130 \\ 5 & 6 & 9 \\ 180 & 1 & 100 \end{bmatrix}$$

10. So we got the original image A_1 .

11. End the image decryption .

5. STATISTICAL PARAMETERS FOR TESTING DIGITAL IMAGES :

Mathematically, it is known that when small changes occur in encrypted operations which tend to large changes of data information leading to good algorithm. The famous image statistical measurements were determined by coefficient correlation (COR), signal peak to noise ratio (PSNR), The number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). It is noted that PSNR based on the number of vanishing moments. Clearly , the attacker may seek to observe variations of the encrypted image in the tiny variations of the plain text to the find correlation between the plaintext and the encrypted image. If a tiny change in the original image can lead to a great change in the image cipher, then the algorithm can resist effectively these differential attacks . Generally, the rate Change of the Number of Pixels (NPCR) and the Average Unified Changing Intensity (UACI) can be used to describe the ability to resist the differential attack. The ideal values of NPCR and UACI are 99.60% and 33.45%, respectively. The four statistical measurements are defined as follows [5] :

$$\mathrm{PSNR} = 10 * \log 10\left(\frac{255 * 255}{\mathrm{MSE}}\right) \quad (13)$$

$$\mathrm{MSE} = \frac{1}{M * N}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(X(i.j) - Y(i.j)\right)^2 \quad (14)$$

$$\mathrm{NPCR} = \frac{\sum D}{M * N} * 100\% \quad (15)$$

$$\mathrm{UACI} = \frac{1}{M * N}\left[\sum \frac{|X - Y|}{255}\right] * 100\% \quad (16)$$

$$\mathrm{COR} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(X(i.j) - E(X)\right)\left(Y(i.j) - E(Y)\right)}{\left[\sum_{i=1}^{N}\sum_{j=1}^{M}\left(X(i.j) - E(X)\right)^2 \sum_{i=1}^{N}\sum_{j=1}^{M}\left(Y(i.j) - E(Y)\right)^2\right]} \quad (17)$$

$$E(X) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(X(i.j) - E(X)\right)}{M * N} \quad (18)$$

Where $D(i.j) = 0$ if $X(i.j) = Y(i.j)$, otherwise $D(i.j) = 1$. X and Y denote the origin image and its corresponding encryption respectively, each with dimension $N * M$.

6. APPLICATION FOR THE PROPOSED ALGORITHM

This algorithm can be applied to the colored digital images. The following is an application of this algorithm to the (Child, floating bridge,Lena, suspended bridge and Baboon) images .

Journal of Theoretical and Applied Information Technology
15th July 2018. Vol.96. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3 Sample Data Base For Five Images, Keys, Cipher-Images, And Images After Decoding.

	Name Image	The origin image	The key image	The encrypted image	The decrypted image
1	Child				
2	floating bridge				
3	Lena				
4	suspended bridge				
5	Baboon				

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

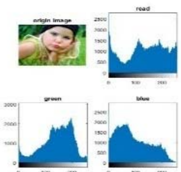
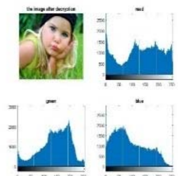
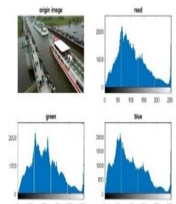
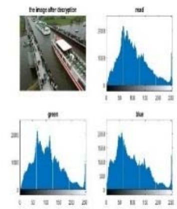
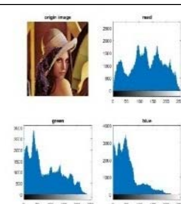
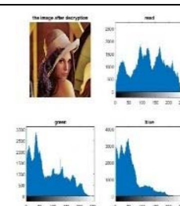
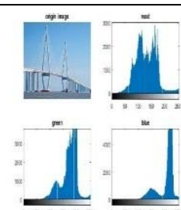
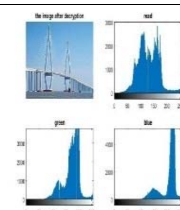
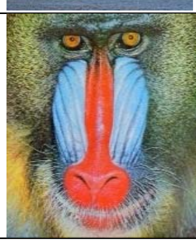
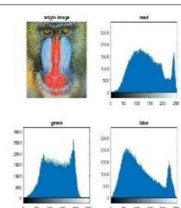
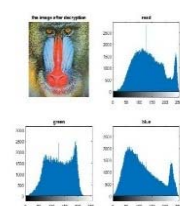
Name Image		Histogram before encryption	Histogram after decryption
Child			
floating bridge			
Lena			
suspended bridge			
Baboon			

Figure 1 Child's, Suspended Bridge, Floating Bridge, Lena, And Baboon Images With Histogram Before Encryption And After Decryption For Each Red, Green And Blue Layer Matrix, With The X-Axis Being Brightness And The Y-Axis Being The Amount Of Pixels.

Journal of Theoretical and Applied Information Technology
15th July 2018. Vol.96. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4. Encryption And Decryption Time, Mean Error, (MSE), (PSNR)

Address of Reading	Name of image				
	Child	floating bridge	Lena	suspended bridge	Baboon
Encryption ime/s	2.9020	2.3400	4.6330	2.2000	4.4770
Decryption ime/s	1 − 32.7780	21.8240	1 − 31.2960	21.8400	28.5010
Mean error	1.6740e − 12	1.7704e − 12	1.9102e − 12	2.1745e − 12	2.7919e − 12
MSE	5.4159e − 23	6.0003e − 23	8.2226e − 23	1.0039e − 22	1.2332e − 22
PSNR	159.4625	159.2399	158.5558	158.1223	157.5241

It appears from Table 4 and through cryptographic and decoding time readings, and standards of accuracy contained in it, especially PSNR exceeding 160 that There is a very large match between the original image and the image after decryption, which confirms the quality of the proposed algorithm.
There is a global statistical accuracy standard used in image research that has been used in our algorithm[6][7]. such as :
The entropy of an image, Standard deviation, for a discrete (the probability density function), Correlation coefficient, NPCR is the number of pixel rate changing, and UACI is the unified changed averaged intensity .
Table 5 shows the comparison between the statistical standards readings pre-encryption and after decryption .It shows that there is no loss of information by virtue of equal readings before and after decryption as shown in Table 5 readings of other statistical standards
Furthermore, table 6 shows a comparison between the readings of encryption and decryption time of our proposed algorithm with other algorithms such as VC (Visual Cryptography) [8]; MK_1-4 (Mohammed al-Kufi—level 1-4) [9]; MK_5[6]; MKA_6[10]; MKHAH_7[11] .

Table 5 . Readings For The Global Standards Accuracy Before Encryption And After Decryption For (Child, Floating Bridge,Lena, Suspended Bridge And Baboon) Images :

Address of Reading	Name of image				
	Child	floating bridge	Lena	suspended bridge	Baboon
Entropy before encryption	0.0741	0.0074	0.1416	1.6775e − 04	0.0030
Entropy after decryption	0.0741	0.0074	0.1416	1.6775e − 04	0.0030
Entropy for encryption image	0	0	0	0	0
Standard deviation before encryption	67.8032	55.4479	63.8309	46.7713	56.1909
Standard deviation after decryption	67.8032	55.4479	63.8309	46.7713	56.1909
Standard deviation for encryption image	5.5897e + 05	4.7958e + 05	5.8884e + 05	4.5143e + 05	4.1175e + 05
Correlation coefficient between original image and image after decryption	1	1	1	1	1
Correlation coefficient between original image and encrypted image	−0.1404	−0.0390	−0.2431	0.4917	0.1233
NPCR	100%	100%	100%	100%	100%
UACI	5.5259e + 05	5.9242e + 05	5.0008e + 05	5.8405e + 05	6.2155e + 05

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 6 . Comparing The Proposed Algorithm With Other Algorithms

Address of Reading	Encryptiontime (Second)	Decryption time (Second)	Encryption time (Second)	Decryption time (Second)
	Name of image			
	Lena	Baboon	Lena	Baboon
MIE [12]	5	9.23	5.16	9.23
MK-1 [6][9]	2.224	2.287	3.11	3.166
MK-2 [6][9]	5.368	5.508	6.013	6.104
MK-3 [6][9]	1.456	1.459	2.138	2.159
MK-4 [6][9]	5.54	5.567	6.265	6.382
MK-5 [6]	2.522	2.338	2.924	3.104
MKA-6 [6]	7.95	8.24	2.13	2.07
MKHAH-7 [6][11]	3.53	3.45	3.57	3.3
MK-8 [6]	1.799	1.898	0.74	0.74
The proposed algorithm	4.6330	4.4770	1 − 31.2960	28.5010

By comparing the proposed algorithm with other algorithms, we note how short the time of encryption and decryption compared to the time of encryption and decryption in other algorithms .

Table 7 . Comparing The Results Of The Global Standards Of Accuracy (MSE) And (PSNR) With Other Works Of Image Processing In General :

Address of Reading	MSE		PSNR	
	Name of image		Name of image	
	Lena	Baboon	Lena	Baboon
MK-1[6][9]	9.9137e − 26	7.9003e − 26	125.0188	125.5118
MK-2[6][9]	9.9137e − 26	7.9003e − 26	125.0188	125.5118
MK-3[6][9]	7.3078e − 27	8.9787e − 27	130.6811	130.2339
MK-4[6][9]	9.9137e − 26	7.9003e − 26	125.0188	125.5118
MK-8[6]	5.0193e − 20	4.4692e − 21	144.6276	149.8797
The proposed algorithm	8.2226e − 23	1.2332e − 22	158.5558	157.5241

It clearly illustrates that our proposed algorithm is excellent in terms of complexity and precision .

7. CONCLUSIONS

Our algorithm (An anew algorithm based on – general singular values decomposition for image cryptography) have the following characteristics which made them a powerful algorithm and it can be adopted in information security :

Combines the GSVD method and the logistics function in encrypting and decoding images.Dependson the GSVD method of encryption and decryption with the logistics function in addition Reduce encryption time and decryption compared with other algorithms. It also depends on the key (real number) in the logistics functionAs well as the key use (image) color in makes it difficult to breakThe algorithm. It is difficult or impossible to be broken beforePirate or unauthorized .This algorithm can also be modified to become a ready algorithm Encrypt texts using the MATLAB program as well. This is an idea for The research project will be submitted later . From Table 4 it is clear that encryption time did not exceed 5.seconds. Also, the decryption time did not exceed 28 seconds. These are the times of record compared to the rest of algorithms. As theglobal standard precision (PSNR) not less than 160 , it is a great read .

REFERENCES

[1] Shah, J. , Saxena , V. , " Performance Study on Image Encryption Schemes " , IJCSI Int. J. Comput. Sci. Issues 2011, 8, 349–355 .

[2] Divya, V.V. , Sudha, S.K. , Resmy , V.R. , " Simple and Secure Image Encryption " , IJCSI Int. J. Comput. Sci. Issues 2012, 9, 286–289 .

[3] Shahram Etemadi Borujeni , Mohammad Saeed Ehsani , " Modified Logistic Maps for Cryptographic Application " , Faculty of Computer Engineering, University of Isfahan, Isfahan, Iran Email.

[4] Hervé Abdi , " Singular Value Decomposition (SVD) and Generalized Singular Value Decomposition (GSVD)" .

[5] Alrammahi A., " Encryption Image Via Mutual Singular Value Decomposition " , World Academy of Science, Engineering and Technology, International Journal of Computer, Information, Systems and Control Engineering Vol:9 No:1, pp. 287- 289, 2015.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[6] Mohammed Abdul Hameed Jassim Al-Kufi , " An a New Algorithm Based on(General Singular Values Decomposition) and (Singular Values Decomposition) for Image Cryptography" , Department of Islamic Education, University of Kufa, 31001 Al-Najaf, Iraq .

[7] Leung, L.W.; King, B. , Vohora, V. , " Comparison of image data fusion techniques using entropy and INI " , In Proceedings of the 22nd Asian Conference on RemoteSensing , Singapore, 5–9 November 2001 .

[8] Sozan , " A. New Visual Cryptography Algorithm for Colored Image " , J. Comput. , 2010 .

[9] Mohammed Abdul- Hameed Jassim Al- Kufi , " Image Encryption with SingularValues Decomposition Aided " , Msc. Thesis to Faculty of Computer Science & Mathematics- University of Kufa- 2014 .

[10] Alrammahi A., Mohammed Al-kufi , " Image Cryptography Via SVD Modular Numbers " , European Journal of Scientific Research Volume 138 No 2 – February, 2016 .

[11] Mohammed Abdul Hameed Jassim Al-Kufi , Hayder Raheem Hashim ,Ameer Mohammed Hussein, and Hind Rustum Mohammed , " An Algorithm Based on GSVD for Image Encryption " , Math. Comput. Appl. 2017, 22, 28; doi:10.3390/mca22020028 .