Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Simulate a first-order Bézier curve in image encoding

Simulate a first-order Bézier curve in image encoding

Mohammed Abdul Hameed Jassim Al-kufi[1], Ola N. Kadhim[2], Eman Saleem Razaq[3],

Department of Mathematics, Basic Education College, University of Kufa, Najaf, Iraq

Al-Furat AL-Awsat Technical University\ Technical Institute of Al-Mussaib

Department of Computer Sciences Faculty of Computer Science & Mathematics, University of Kufa

mohammeda.alkufi@uokufa.edu.iq, ola.najah@atu.edu.iq, saleememan0@gmail.com

Abstract. Bézier curve of the first rank is a simple equation in terms of form, but it is characterized by the nature of private transactions making it difficult to use in image encryption because the dispersion of color values is not enough, this results in an encrypted image that gives clear references to the original image. This weakness in the equation does not exist in the case of text encryption where enough to change the numerical values of the components of the text to get a digital matrix representing the encrypted text.Through this algorithm we have used the Bézier curve technique from the first order of image coding we used a new method to generate the coefficients of the equation where we simulated the Bazier equation where it became as follows:

- y=x_1*(t-1)+x_2*t

- Where 0<t<1

To illustrate the work of this technology in image encoding the core of our work is in choosing a vector (1 × 4) with four numerical components)k_1,k_2,k_3,k_4 (So that k_1<k_2 and k_3 <k_4 , k_1 and k_2 have the same signal, as well as k_3 and k_4 also have the same reference to give them t_1 and t_2 Where t_1=k_1/k_2 and t_2=k_3/k_4 which will ensure that both have t_1 and t_2 have positive values less than 1. We have thus designed the equation of Bézier curve suitable for a scattering of color values of the image process, as well we'll see it by explaining the way in detail below and tables of readings and global standards that have been inferred by the application of the algorithm

Keywords- encryption; Bézier curve from ONE ORDER; image encryption.…

1. Introduction

It is no secret to anyone. Encrypt information and hide data it is from the ancient sciences that the nations raced to develop their skills in this aspect. This science is a field of applied mathematics we use modern, sophisticated algebraic mathematical methods in distracting the color values of the image. In the same way with radical modulation we encode texts. We have developed a new method of encryption in line with the tremendous development of computer science and informatics. We have taken a new approach to encryption it converts the image we want to encode or the text we want to encode into a numerical array where there is no intimation to the image or text, after the old encryption algorithms were keen to be encrypted image is converted to another image. And encrypt the text is converted to text other than the concept.

This method has become the past where we have developed our new method during our previous research as we have mentioned above to convert the object we encode into a digital matrix is impossible to break.

Below are examples of the development of image and text encryption algorithms that we accomplished during our research career which will be part of the algorithms that we will compare the results of this algorithm: -

1. Algorithm (MK-1): It is an algorithm through which the use of a matrix analysis (SVD) for the first time in the image encryption using real numbers as encryption keys. This algorithm was a new transition in cryptography where through which to deal with the matrix color values of the image and dispersed to other matrix do not refer to the original matrix.
2. Algorithm (MK-2): It represents the first development of the MK-1 algorithm. Through which we increase the complexity of the dispersion of the values of color process making encryption difficult to break.
3. Algorithm (MK-3): It represents the second development of the MK-1 algorithm. Further complexity has been added to the MK-2 algorithm. Make encryption more complex.
4. Algorithm (MK-4): We did not stop increasing the complexity of encryption for the sake of maximum information immunity complexity rings were added to the MK-3 algorithm. To access the algorithm (MK-4) which represents an advanced stage of development of the original algorithm (MK-1). All of these algorithms (MK-1), (MK-2), (MK-3), and (MK-4) basically based on matrix analysis (SVD). It possesses very high flexibility that helps in the processing and encryption of images as well as texts.
5. Algorithm (MK-5): It is an algorithm that we used to implement the same mathematical tool (SVD) but the method is different in essence, it is considered a new development in the world of encryption. The results were competing in previous algorithms.
6. Algorithm (MKA-6): It's a new algorithm that combines (SVD) with (Modular Numbers), it became a complex coding of color values. Which added a new complex encryption make broken very difficult or impossible.
7. Algorithm (MKHAH-7): It is an entirely new algorithm where we used the new technology for the first time in the world, it is a matrix analysis technique (GSVD) through which we used an image as an encryption key, we put the key and image we want to encrypt to GSVD to extract this last matrix represents the original image encryption ... This technique represented a qualitative leap in the science of encryption in terms of using the image as an encryption key, the distracting force at work, and the accuracy of the results and lack of error in the work.
8. Algorithm (MK-8): In this algorithm we have taken the greatest complexity in the dispersion of the color value matrix of the image we want to encode in this algorithm we have combined two technologies, SVD and GSVD. For the first time in the world these two technologies are combined. For the purpose of applying these two techniques, we used two encryption keys. The first is a real number for the first stage in encryption (SVD). The second key is an image which is specific to GSVD technology, Readings have proven to global standards of accuracy that resulted from the work and the application of this algorithm vehicle that the algorithm is very excellent and the error rate is very small.
9. Algorithm (MK-9): A new algorithm in its principle but it is very similar to the algorithm (MK-6) where we used the technique here (GSVD) and (Modular Numbers), where we used a different key from the one used in SVD and (Modular Numbers). The key used in the MK-6 algorithm it was a real number and with it the key to (modular numbers). But in the algorithm (MK-9) the encryption key for (GSVD) is an image to which the key is added (Modular Numbers). This algorithm represents an update of the previous algorithms and to develop the dispersion methods that we used in cryptographic algorithms.

All of these algorithms have been successive phases of our research and are developing one another.

We add some other global algorithms which we used the results of which comparisons tables between the readings of global standards of accuracy and is as below: -

1. Algorithm (SKM-JPEG).
2. Algorithm (SKM-BPP).
3. Algorithm (NKP).
4. Algorithm (DSA).
5. Algorithm (TTS).
6. Algorithm (AZA).
7. Algorithm (NDD).

Encryption is not just about the algorithms we mentioned above since this science develops daily and even every hour in terms of the number of workers in this important scientific field of professors, researchers and students.

2. The accuracy criteria used during this research:

For the purpose of clarifying the quality and accuracy of the work, small error in the result during work, encryption time and decoding time. Some global statistical standards have been used.

Adopted through image processing algorithms and information encryption. We relied on previous research () to develop summaries of the names of those standards, as follows: -

1[EBE]: Entropy before encryption.
2[EAD]: Entropy after decryption.
3[EEI]: Entropy for encryption image.
4[SDBE]: Standard deviation before encryption.
5[SDAD]: Standard deviation after decryption.
6[SDEI]: Standard deviation for encryption image.
7[CCOAD]: Correlation coefficient between original image and image after decryption.
8[CCOE]: Correlation coefficient between original image and encrypted image.

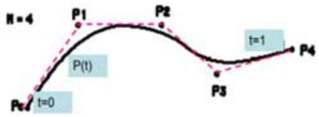
In this that our algorithm denoted by the symbol (MK-10) we will use the technology (first-order Bézier curve) to dispersion of the color values of the image matrix. To know this vast and complex technical, in the next section we will touch on something brief.

3. Bézier curve:-

We are as usual in the former our research clarify something brief about every technique we use in our algorithm we refer to the sources as possible return to it for more information about Bézier curve. We will cut short talk about them and avoid going into the details and types.

[redacted]*Definition*

Bezier Curve P (t) is a continuous function in 3 space defining the curve with N discrete control points B_i . t=0 at the first control point (i=0) and t=1 at the last control point (i=N).



Bezier Curve: A Bezier Curve is obtained by a defining polygon.

Application: Where aesthetic appeal is more important than accuracy. Sometimes functional requirements demand such a curve. Ab initio designs may need such curves.

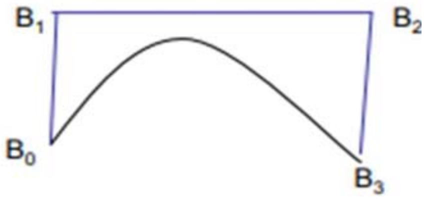
$$P(t) = \sum_{i=0}^{n} B_i J_{n,i}(t)$$

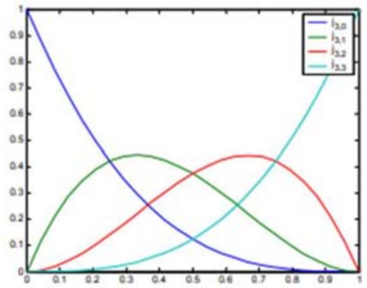
And $J_{n,i}(t) = \frac{n!}{i!(n-i)!} t^i (1-t)^{n-i}$

For example

$J_{3,0}(t) = (1-t)^3$

$$J_{3,1}(t) = 3t(1-t)^2$$
$$J_{3,2}(t) = 3t^2(1-t)^1$$
$$J_{3,3}(t) = t^3$$
$$\therefore P(t) = B_0 J_{3,0}(t) + B_1 J_{3,1}(t) + B_2 J_{3,2}(t) + B_3 J_{3,3}(t)$$
$$= (1-t)^3 P_0 + 3t(1-t)^2 P_1 + 3t^2(1-t)^1 P_2 + t^3 P_3$$





[redacted] *Properties of the basis function*

- The curve in general does not pass through any of the control points except the first and last. From the formula $P(0) = B_0$ *and* $P(1) = B_n$
  $$J_{n,0}(0) = \frac{n!(0)^0(1-0)^{n-0}}{n!} = 1 \qquad i = 0$$
  $$J_{n,i}(0) = \frac{n!\,(0)^i(1-0)^{n-i}}{i!\,(n-i)!} = 0 i \neq 0$$
  $$\therefore \; P(0) = B_0 J_{n,0}(0) = B_0$$
- The curve in general does not pass through any of the control points except the first and last. From the formula $P(0) = B_0$ *and* $P(1) = B_n$
  $$J_{n,n}(1) = \frac{n!(1)^n(0)^{n-n}}{n!(1)} = 1 \qquad i = n$$
  $$J_{n,i}(1) = \frac{n!\,(1)^i(0)^{n-i}}{i!\,(n-i)!} = 0 \qquad i \neq n$$
  $$\therefore \; P(1) = B_n J_{n,n}(1) = B_n$$
- For any given value of the parameter t, the summation of the basis functions is exactly equal to 1 i.e.,
  $$\sum_{i=0}^{n} J_{n,i}(t) = 1$$
- The curve is always contained within the convex hull of the control points, it never oscillates wildly away from the control points.
- If there is only one control pointB_0, ie: n=0 then P (t) = B_0 for all t.
- If there are only two control points P_0 andP_1, ie: n=1 then the formula reduces to a line segment between the two control points.
- The blending function is always a polynomial of degree one less than the number of control points.
- Thus 3 control points result in a parabola, 4 control points a cubic curve etc.

- Closed curves can be generated by making the last control point the same as the first control point.
- First order continuity can be achieved by ensuring the tangent between the first two points and the last two points are the same.
- Adding multiple control points at a single position in space will add more weight to that point "pulling" the Bézier curve towards it.

[redacted]*Maximum value of Blending functions*

- It is observed that the blending functions are quite symmetric in nature.
- The maximum value occurs at:

$$max\big(J_{n,i}(t)\big) = \frac{d\big(J_{n,i}(t)\big)}{dt} = 0 \quad t = ?$$

$$max\big(J_{n,i}(t)\big) = J_{n,i}\left(\frac{i}{n}\right) = \mathrm{C}_i^n\,\frac{i^i(n-i)^{n-i}}{n^n}$$

$$E.g.\ \ J_{3,1}\left(\frac{1}{3}\right) = ?$$

$$J_{3,2}\left(\frac{2}{3}\right) = ?$$

$$Ans\ \ J_{3,1}\left(\frac{1}{3}\right) = \frac{4}{9}$$

$$J_{3,2}\left(\frac{2}{3}\right) = \frac{4}{9}$$

Suffice to this extent clarify Profile of (Bézier curve)

4. Methodology of proposed algorithm of encryption and decryption:

We will explain the algorithm through a hypothetical example:

Let A be an origin image matrix

$$\mathrm{A} = \begin{bmatrix} 22 & 45 \\ 78 & 25 \end{bmatrix}$$

let k be an (1×4) matrix (key) in which k(1)<k(2) and k(3)<k(4)

$$\mathrm{k} = [12 \quad 25 \quad 23 \quad 88]$$

Encryption:

$$\mathrm{encA} = \begin{bmatrix} \mathrm{A}(1,1) * \left(\frac{\mathrm{k}_1}{\mathrm{k}_2} - 1\right) + \mathrm{A}(1,2) * \frac{\mathrm{k}_1}{\mathrm{k}_2} & \mathrm{A}(1,1) * \left(\frac{\mathrm{k}_3}{\mathrm{k}_4} - 1\right) + \mathrm{A}(1,2) * \frac{\mathrm{k}_3}{\mathrm{k}_4} \\ \mathrm{A}(2,1) * \left(\frac{\mathrm{k}_1}{\mathrm{k}_2} - 1\right) + \mathrm{A}(2,2) * \frac{\mathrm{k}_1}{\mathrm{k}_2} & \mathrm{A}(2,1) * \left(\frac{\mathrm{k}_3}{\mathrm{k}_4} - 1\right) + \mathrm{A}(2,2) * \frac{\mathrm{k}_3}{\mathrm{k}_4} \end{bmatrix}$$

$$\mathrm{encA} = \begin{bmatrix} 22 * \left(\frac{12}{25} - 1\right) + 45 * \frac{12}{25} & 22 * \left(\frac{23}{88} - 1\right) + 45 * \frac{23}{88} \\ 78 * \left(\frac{12}{25} - 1\right) + 25 * \frac{12}{25} & 78 * \left(\frac{23}{88} - 1\right) + 25 * \frac{23}{88} \end{bmatrix}$$

$$\mathrm{encA} = \begin{bmatrix} 10.16 & -4.4886364 \\ -28.56 & -51.079545 \end{bmatrix}$$

Decryption:

Encryption image is

$$\mathrm{encA} = \begin{bmatrix} 10.16 & -4.4886364 \\ -28.56 & -51.079545 \end{bmatrix}$$

Encryption key is

$$\mathrm{k} = [12 \quad 25 \quad 23 \quad 88]$$

$$\frac{encA(1,2)-\frac{encA(1,1)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}{\left(\frac{k_3}{k_4}-1\right)-\frac{\left(\frac{k_1}{k_2}-1\right)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}} \quad \frac{encA(1,1)-\frac{encA(1,2)-\frac{encA(1,1)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}{\left(\frac{k_3}{k_4}-1\right)-\frac{\left(\frac{k_1}{k_2}-1\right)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}*\left(\frac{k_1}{k_2}-1\right)}{\frac{k_1}{k_2}}$$

$$\frac{encA(2,2)-\frac{encA(2,1)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}{\left(\frac{k_3}{k_4}-1\right)-\frac{\left(\frac{k_1}{k_2}-1\right)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}} \quad \frac{encA(2,1)-\frac{encA(2,2)-\frac{encA(2,1)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}{\left(\frac{k_3}{k_4}-1\right)-\frac{\left(\frac{k_1}{k_2}-1\right)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}*\left(\frac{k_1}{k_2}-1\right)}{\frac{k_1}{k_2}}$$

And for more clarification:-

$$A(1,1)=\frac{encA(1,2)-\frac{encA(1,1)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}{\left(\frac{k_3}{k_4}-1\right)-\frac{\left(\frac{k_1}{k_2}-1\right)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}$$

$$A(1,2)=\frac{encA(1,1)-\frac{encA(1,2)-\frac{encA(1,1)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}{\left(\frac{k_3}{k_4}-1\right)-\frac{\left(\frac{k_1}{k_2}-1\right)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}*\left(\frac{k_1}{k_2}-1\right)}{\frac{k_1}{k_2}}$$

$$A(2,1)=\frac{encA(2,2)-\frac{encA(2,1)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}{\left(\frac{k_3}{k_4}-1\right)-\frac{\left(\frac{k_1}{k_2}-1\right)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}$$

$$A(2,2)=\frac{encA(2,1)-\frac{encA(2,2)-\frac{encA(2,1)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}{\left(\frac{k_3}{k_4}-1\right)-\frac{\left(\frac{k_1}{k_2}-1\right)*\frac{k_3}{k_4}}{\frac{k_1}{k_2}}}*\left(\frac{k_1}{k_2}-1\right)}{\frac{k_1}{k_2}}$$

$$\therefore\ \mathrm{A}=\begin{bmatrix}22 & 45\\ 78 & 25\end{bmatrix}$$

5. Application for the proposed algorithm:

This algorithm is very flexible. It can be applied to all kinds of image. It can also be applied to encrypt text and symbols in all languages. Therefore, our subsequent research will focus on the encoding of texts, through modification of this algorithm and previous algorithms in making the error in the results is equal to zero, because text encryption is not likely any error in restoring the results.

Below are tables of readings and a figure for the results we obtained through programming algorithm by MATLAB program, has applied them to three images are Baboon, Lena and the girl child.

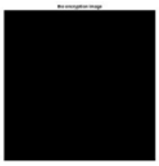
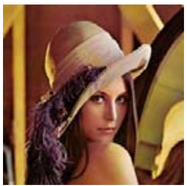
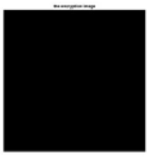
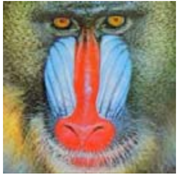
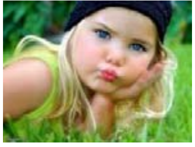
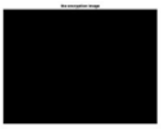
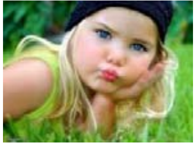
Image Name	The original image	Encryption key	Cipher- image by Bézier curve	Image after decoding
Lena		810 12345 9000 100000		
Baboon		987 12345 213 90987		
Child		908 76543 12 908		

Figure 1. Sample Data Base for three images, Keys, cipher-images, and Images after decoding

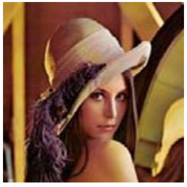
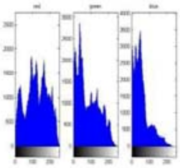
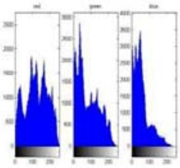
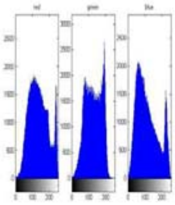
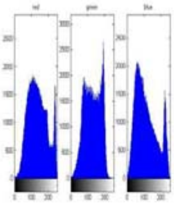
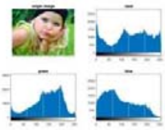
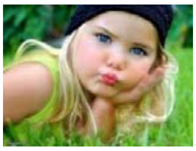
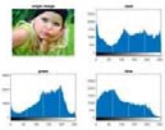
Image Name	The original image	Histogram before encryption	Image after decoding	Histogram after decryption
Lena				
Baboon				
Child				

Figure 2: three Images of Lena, Baboon and child with histograms of each other before encoding and after decoding

Note the results match in the three pictures above where the great similarity between the original image and the image after decoding and histogram match before and after decoding. As we will notice in the subsequent tables the power of the algorithm through the readings that appeared to us for the time of encryption and decoding time and readings of global statistical accuracy standards. These privileges make us say that the algorithm is very excellent and very powerful and hackers cannot penetrate it.

6. Experimental result

From figures 1 and 2, is clear to us exact match between the original image and the image after decoding. As is also evident from histogram matching. We do not hesitate to say that this algorithm is good and characterized by the rest of the algorithms.

Table 1. Encryption and decryption time, Mean error, (MSE)*&* $(PSNR)^*$ *for (Baboon, Lena, and child) images.*

Name of Image	Encryption time/s	Decryption time/s	Mean error	MSE	PSNR
Baboon	0.5580	0.5970	6.2420e-14	1.4184e-26	177.3719
Lena	0.5650	0.6090	1.7347e-13	1.2532e-25	172.6407
Child	0.5300	0.5430	4.4714e-12	7.5781e-23	158.7330

Very clear from the table (1) that the encoding time and the decoding time are very acceptable, As well as the case of readings accuracy standards contained in the same table it is very acceptable compared to other readings if we take into account the accuracy and complexity of the algorithm that exceeded expectations.

Not satisfied with what stated in Table 1 above the statistical standards for measuring accuracy. Rather, we took readings of other criteria that were taken into account in the previous algorithms. We have listed in table (2) below, these criteria are:

1. Entropy of the image.
2. Standard deviation, for a separate divider (the probable density function).
3. Correlation coefficient.
4. The tone of the change of the pixel rate.
5. WSI is the average of variable intensity.To understand these statistical criteria, the research can be reviewed.

Table 2 shows no data loss after decoding, due to equal readings before and after decoding this is a clear indication of the quality of this algorithm.

Name of Image	EBE(*)	EAD(*)	EEI(*)	SDBE(*)	SDAD(*)	SDEI(*)	CCOAD(*)	CCOE(*)	NPCR	UACI
Baboon	0.0030	0.0030	7.1351e-04	56.1909	56.1909	52.9138	1	-0.9287	99.9822	95.1084
Lena	0.0741	0.0741	0.0509	67.8032	67.8032	66.0972	1	-0.9960	99.4955	95.7782
child	0.0741	0.0741	0.0509	67.8032	67.8032	66.0972	1	-0.9960	99.4955	95.7782

(*) We have shown these symbols and what they indicate at the beginning of the research at the introduction.

In Table 3 below, we compare the encoding time and decoding time of our MK-10 algorithm. with the last four algorithms previous to us are:

- MKA-6[13].
- MKHAH-7[7].
- MK-8[17]
- MK-9[17]

Table 3. Comparing the proposed algorithm with our last four algorithms for only two image (Lena and Baboon)

Algorithm		MKA-6	MKHAH-7	MK-8	MK-9	Our algorithm MK-10
Image	Lena	7.95	3.53	1.799	3.35	0.5650

Encryption time (Second)		Baboon	8.24	3.45	1.898	3.46	0.5580
Decryption Time (Second)	Image	Lena	2.13	3.57	0.73	3.35	0.6090
		Baboon	2.07	3.3	0.74	3.43	0.5970

In Table (4) below is a comparison between two criteria (MSE) and (PSNR) between this algorithm and our last four algorithms.

Table 4. Comparing the results of the global standards of accuracy (MSE) and (PSNR) with other works of image processing in general..

Algorithm			MKA-6	MKHAH-7	MK-8	MK-9	Our algorithm MK-10
MSE	Image	Lena	0	7.8839e-30	5.0193e-20	1.9491e-006	1.2532e-25
		Baboon	0	***	4.4692e-21	3.8846e-006	1.4184e-26
PSNR	Image	Lena	Inf	145.5163	144.6276	28.5598	172.6407
		Baboon	Inf	***	149.8797	27.1084	177.3719

(***) means that the address is not calculated

7. Conclusions:

We took care of this algorithm (Simulate a first-order Bézier curve in image encoding) on the sobriety dispersing image matrix through a complex cryptographic key which is a vector with certain specifications, making it difficult to break the encryption. This algorithm is considered to be a significant development of the previous algorithms, it is ready for application in the areas of security.

In addition, this algorithm is a template ready to be applied to text encryption in all languages. The advantages of this algorithm can be summarized as follows:

1. The work represents a distinct encryption strength and is difficult to break.
2. A complex encryption key that is a vector of four real numbers, it is specific key is a complex key that makes the algorithm with its distinctive horse.
3. The algorithm is ready to encrypt all kinds of images without exception.
4. The algorithm is a template ready to encode texts in all languages.
5. Encoding time and decryption time are very ideal. They are so small that they gave a special feature to this algorithm as shown in Table (1).
6. There is no missing or error in data recovery, this is clear from the nature of the relationship between the original image and the image after decoding is equal to (1).

8. Discussion:

1. This algorithm (Simulate a first-order Bézier curve in image encoding) is an entirely different from previous algorithms used the same (Bézier curve) in terms of the method used in encryption.
2. Is possible to combine this algorithm and any previous algorithm to increase the complexity of the dispersal of the image, and this is our future project research.

3. The coding time and decoding time given in the tables above are not final. They depend on the version of MATLAB used and the speed of the user's computer. Therefore, the recorded time can be reduced if we use another version and a faster computer.
4. In accordance with our method of image encryption or text encryption we have converted the image into a numerical matrix encrypted. Contrary to what was in place previously when
5. Encryption is to convert the image to another image.
6. Statistical criteria used to measure the accuracy of the algorithm is a global standards. The researchers were able to make comparisons between their later work and this algorithm.
7. The algorithm succeeded in its application testing by MATLAB on all kinds of pictures so that the beneficiaries can use them immediately upon agreement with us.

9. Acknowledgments

At the end of this research we can only thank the Miss (Fayhaa Majeed Hamid . Mathematics Teacher in Zain Al-Abidin School for Boys affiliated to the Directorate of Education of Kufa in Najaf,For the assistance extended to us in taking out this research in its current form Through their available means, Where provided everything you can from logistical aid including us helped speed the completion of this research.

References

[1] "FreeType Glyph Conventions / VI. FreeType outlines" (http://www.freetype.org/freetype2/docs/glyphs/glyphs-6.html). The Free Type Project. 13 February 2018. "FreeType Glyph Conventions – Version 2.1 / VI. FreeType outlines" (https://web.archive.org/web/20110929201958/http://www.freetype.org/freetype2/docs/glyphs/glyphs-6.html). 6 March 2011. Archived from the original (http://www.freetype.org/freetype2/docs/glyphs/glyphs-6.html) on 2011- 09-29.

[2] Adil AL-Rammahi& Mohammed Al-kufi; Image Cryptography Via SVD Modular Numbers; European Journal of Scientific Research- Volume 138 No 2 - February, 2016

[3] Amira B. S., Zahraa M. T. Ahmed S. N. 2010. An Investigation for Steganography using Different Color System. Rafidain Journal of Computer Science and Mathematics for the year. Proceedings of the Third Scientific Conference on Technology of information. 29-30 / Nov. / 2010, Faculty of Computer Science and Mathematics - University of Mosul. :474-492:" http://computerscience.uomosul.edu.iq/files/pages/page_4034788.pdf"

[4] Biswas, Pradipta; Langdon, Pat (2015-04-03). "Multimodal Intelligent Eye-Gaze Tracking System". International Journal of Human-Computer Interaction. 31 (4): 277–294. doi:10.1080/10447318.2014.1001301 (https://doi.org/10.1080%2F10447318.2014.1001301). ISSN 1044-7318 (http s://www.worldcat.org/issn/1044-7318).

[5] Deepak A., Sandeep K., Anantdeep A. 2010. An Efficient Watermarking Algorithm To Improve Payload And Robustness Without Affecting Image Perceptual Quality, Journal of Computing.2(4). 105-109

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

[7] Duncan Marsh (2005). Applied Geometry for Computer Graphics and CAD. Springer Undergraduate Mathematics Series (2nd ed.). ISBN 978-1- 85233-801-5. ASIN 1852338016 (https://www.amazon.co.uk/dp/1852338016).

[8] G.A.Sathishkumar ,Dr.K.Bhoopathy bagan and Dr.N.Sriraam; Image Encryption Based On Diffusion And Multiple Chaotic Maps; International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011

[9] Gerald E. Farin; Josef Hoschek; Myung-Soo Kim (2002). Handbook of Computer Aided Geometric Design (https://books.google.com/books?id=0S V5G8fgxLoC&pg=PA4). Elsevier. pp. 4–6. ISBN 978-0-444-51104-1.

[10] Hansen, P.C. Regularization, GSVD and truncated GSVD. BIT Numer. Math. 1989, 29, 491–504.

[11] Hazewinkel, Michiel (1997). Encyclopaedia of Mathematics: Supplement (https://books.google.co.uk/books?id=3ndQH4mTzWQC&pg=PA119). 1. Springer Science & Business Media. p. 119. ISBN 9780792347095.

[12] John Burkardt. "Forcing Bezier Interpolation" (https://web.archive.org/web/20131225210855/http://people.sc.fsu.edu/~jburkardt/html/bezier_interpo lation.html). Archived from the original (http://people.sc.fsu.edu/~jburkardt/html/bezier_interpolation.html) on 2013-12-25.

[13] M. Macq .,J.-J. Quisquater., : Cryptology for digital TV broadcasting. Proceedings of the IEEE, Vol. 83, No. 6, pp. 944–957 (1995)

[14] M. Yang., N. Bourbakis., L. Shujun. : Data-image-video encryption. Potentials, IEEE, vol. 23, pp. 28-34, (2004)

[15] Mark Kilgard (April 10, 2012). "CS 354 Vector Graphics & Path Rendering" (http://www.slideshare.net/Mark_Kilgard/22pathrender). p. 28.

[16] MATLAB Version 7.12.0.635 (R2011a) 32 bit (win 32) march 18,2011 License Number 161052.

[17] Max K. Agoston (2005). Computer Graphics and Geometric Modelling: Implementation & Algorithms (https://books.google.com/books?id=TAYw3L Es5rgC&pg=PA404). Springer Science & Business Media. p. 404. ISBN 978-1-84628-108-2.

[18] Mohammed Abdul- Hameed Jassim Al- Kufi; Image Encryption with Singular Values Decomposition Aided; Msc. Thesis to Faculty of Computer Science & Mathematics- University of Kufa- 2014

[19] Mohammed Abdul- Hameed Jassim Al- Kufi; text and image encryption via text and image keys using singular values decomposition; international journal of engineering and future technology-volume 1;issue No. 1; year 2016- ISSN 2455-6432

[20] 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 www.mdpi.com/journal/mca

[21] Mohammed Abdul Hameed Jassim Al-Kufi; An a New Algorithm Based on (General Singular Values Decomposition) and (Singular Values Decomposition) for Image Cryptography; Elixir Digital Processing 114 (2018) 49604-49609

[22] Mohammed Abdul Hameed Jassim Al-Kufi;" IMAGE ENCRYPTION & DECRYPTION VIA (GSVD-MODULAR NUMBERS)"; Journal of Engineering and Applied Sciences; Vol 13(21) 9194-9203 2018

[23] Mortenson, Michael E. (1999). Mathematics for Computer Graphics Applications (https://books.google.co.uk/books?id=YmQy799flPkC&pg=PA26 4). Industrial Press Inc. p. 264. ISBN 9780831131111.

[24] Narendra K P. 2012. Image encryption using chaotic logistic map, ELSEVIER. 24(9).: 926-934

[25] Nidhal K. El Abbadi, Adil Mohamad and Mohammed Abdul-Hameed, IMAGE ENCRYPTION BASED ON SINGULAR VALUE DECOMPOSITION, Journal of Computer Science, Vol 10 (7): 1222-1230, 2014

[26] Rida T. Farouki. "Introduction to Pythagorean-hodograph curves" (http://faculty.engineering.ucdavis.edu/farouki/wp-content/uploads/sites/41/2013/ 02/Introduction-to-PH-curves.pdf) (PDF)., particularly p. 16 "taxonomy of offset curves".

[27] S. Parker., L. O. Chua., :Chaos: a tutorial for engineers. Proceedings of the IEEE, Vol. 75, No. 8, pp. 982–1008 (1995)

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

[29] Shaimaa A., Khalid F. A., Mohamed M. F. 2011. Securing Image Transmission Using In-Compression Encryption Technique. International Journal of Computer Science and Security, (IJCSS), 4(5): 466-481

[30] Shene, C.K. "Finding a Point on a Bézier Curve: De Casteljau's Algorithm"

(http://www.cs.mtu.edu/~shene/COURSES/cs3621/NOTES/spline/Bezi er/de-casteljau.html). Retrieved 6 September 2012.

[31] Sozan, A. New Visual Cryptography Algorithm for Colored Image. J. Comput. 2010, 2, 4

[32] Teofilo Gonzalez; Jorge Diaz-Herrera; Allen Tucker (2014). Computing Handbook, Third Edition: Computer Science and Software Engineering (htt ps://books.google.com/books?id=vMqSAwAAQBAJ&pg=SA32-PA14). CRC Press. page 32-14. ISBN 978-1-4398-9852-9.

[33] Trinadh T., Venkata N. 2012. A Novel PSNR-B Approach for Evaluating the Quality of De-blocked Images. IOSR Journal of Computer Engineering. 4(5).: 40-49

[34] W.Wu .,N. F. Rulkov., :Studying chaos via 1-Dmaps—a tutorial. IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications, vol. 40, no. 10, pp. 707–721 (1993)

[35] W.Wu .,N. F. Rulkov., :Studying chaos via 1-Dmaps—a tutorial. IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications, Vol. 40, No. 10, pp. 707–721 (1993)

[36] Wei, Y.; Xie, P.; Zhang, L. Tikhonov regularization and randomized GSVD. SIAM J. Matrix Anal. Appl. 2016, 37, 649–675.

[37] Wells, John (3 April 2008). Longman Pronunciation Dictionary (3rd ed.). Pearson Longman. ISBN 978-1-4058-8118-0.

[38] Yi, C. H. Tan., C. K. Siew., R. Syed.,: Fast encryption for multimedia. IEEE Transactions on Consumer Electronics, vol. 47, no. 1, pp. 101–107 (2001)A reference