

PAPER • OPEN ACCESS

An Image of Encryption Algorithm Using Graph Theory and Speech Signal Key Generation

To cite this article: Iman Qays Abduljaleel *et al* 2021 *J. Phys.: Conf. Ser.* **1804** 012005

View the [article online](#) for updates and enhancements.



EEG/ECOG AMPLIFIERS
& ELECTRODES
ELECTRICAL/CORTICAL
STIMULATORS
REAL-TIME PROCESSING

g.tec
gtec.at/shop
SHOP NOW

An Image of Encryption Algorithm Using Graph Theory and Speech Signal Key Generation

Iman Qays Abduljaleel¹, Samaher Adnan Abdul-Ghani², Huda Zaki Naji³

¹Computer Science Department, College of Computer Science and Information Technology, Basrah, Iraq.

^{2,3}Department of Mathematics, College of Sciences, University of Basrah, Al- Basrah, Iraq.

emankais@yahoo.com

samaheradnanmath@gmail.com

samaher.adnan@uobasrah.edu.iq

hudazaki4@gmail.com

Abstract. In this paper, a color image of encryption algorithm used a graph theory has been proposed. The proposed algorithm depends on the audio files as a basis for exploiting a set of keys for encoding color images. The key generation system was built by passing the audio signal in several stages based on the graph theory. The results revealed that the proposed algorithm has generated the encrypted images with uniform distribution in pixel histograms with information entropy closes to 8, which resists different attacks. The comparison experiments with other recent algorithms were performed. The statistical results show that the proposed algorithm has a strong security against attacks.

Keywords. Image encryption, Graph theory, Scrambling, Speech, Arnold's Transform.

1. Introduction

The transfer of photos, videos and multimedia with private or commercial information has become of great importance especially with the development of network technology and digital multimedia services. These technologies provide many methods to exchange/transfer information and data between people around the world. For example, video surveillance networks allow remote video monitoring for internal security purposes and also facilitate the transmission and sharing of video clips and image data. Therefore, the deployment of video surveillance systems in important areas such as airports, malls, banks, schools, and even military locations, results in the transportation and storage of large quantities of videos and photos with safety information. Therefore, providing security for multimedia information becomes a necessary for government and private companies as well as for individuals [1]. In many areas, the protection and security of information are very important for example privacy, video surveillance for internal security, copyright protection and security communication in military applications.

Multimedia Cryptography can make the multimedia data difficult for unauthorized users to decode by transferring the multimedia data into a completely different format [2,3]. The field of encryption is



concerned with developing tools and techniques for the hiding of messages, information, or data so that it can't be detected by unintended parties. The overall objective of encryption is to prevent information from being stolen, lost, destroyed by an attacker, modified, or otherwise discovered by unintended recipients [3,4]. This is accomplished by making the communication a part of some other medium, or carrier, so that an unaware observer will not be able to detect that there is a message present [7, 10]. The message is "hiding in plain sight" inside a seemingly innocent medium, and should remain hidden so long as nobody is looking for it. The intended recipient, however, can reveal the message using knowledge of both its presence inside a medium and the method used to conceal it. The demand for steganography tools has grown over time, as the need for secure communication has increased proportionally with the amount of data that society exchanges [9]. There are legitimate uses for steganography, such as copyright protection, circumvention of web surveillance and censorship in areas of the world where data flow is restricted, and in U.S. military and intelligence communications [7]. There are also many illegitimate uses, including that in organized crime, human trafficking, terrorism, child exploitation, espionage, and data exfiltration from enterprise networks [6].

Most of previous research uses the chaotic to generate the keys. This method is despite its ease, but due to its frequent use it has become easier to predict the encrypted keys by others. This research uses graph theory to generate the keys. One of the advantages of generating keys by the graph theory: allows the generation of keys to be difficult to predict by others, specificity to the sending person as well as it is characterized by speed and randomness. The paper is organized as follows. A related work gives in section 2. The proposed algorithm presents in section 3 includes. The experiment results present in section 4. Section 5 gives the conclusions of the paper.

2. Related Work

2.1. Arnold's Transform

Arnold's Transform is a type of periodic chaotic map which is used to create randomness in the signal when applied to the signal. Here Arnold's transform is achieved using the following matrix equation:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N$$

Where (x', y') represents the new position of the pixel, whereas the (x, y) represents the original position of the pixel. Here N indicates to the order or a size of an image matrix. To perform Arnold's Transform, the two-dimensional signal is iterated times using the above equation. As Arnold's Transform is periodic in nature, the original image is retrieved after a specific number of iterations T . The value of T varies with the size of the matrix. Here Figure 1.(b), 1.(c) and 1.(d) represents images obtained after iterating the image in the Figure 1.(a) with Arnold's transform. From the figure 1. (d) we can confirm that Arnold's transform is periodic in nature.

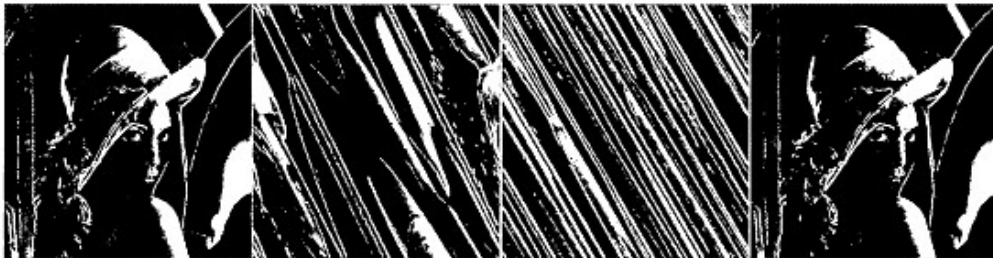


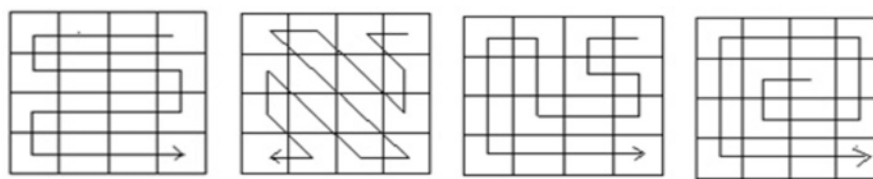
Figure 1. Examples of an Image subjected to Arnold's Transform, (a) Original Image, (b) Image obtained after 1st iteration, (c) Image obtained after 2nd iteration, (d) Image obtained after 384th iteration.

2.2. *Biometrics- Based Cryptographic Key Generation*

Encryption keys are widely utilized to control when access to bank accounts or computing resources as in ATM, also to validate user authenticity in e-business. Generally, the randomness chosen or user-defined system PINs and passwords are used to create unique access control keys. However, a random key is easy to forget, and user-specified key is vulnerable to dictionary attacks and is easy to move. Biometrics, for example, the face, sound, iris, and fingerprints, contribute to specific characteristics for all individual. Thus, the biometric data may potentially be taken as a supplement for PINs and passwords [12,13]. Given the fact that the combination of biometrics and coding can give the best of both worlds, it has become a focus of attention for many researchers [14]. In information transactions over communication networks, encryption guarantees a high degree of confidence, while biometrics ensure a high degree of certainty when individuals are identified as based on a scale of their personal characteristics [15,16].

2.3. *Basic Scanning Methodology*

A combined system of compression, coding, and hiding that was proposed by Bourbakis in 1986 as this system is based on the SCAN language. The word "SCAN" refers to the different methods of scanning a two-dimensional image [18]. The SCAN language can produce a(mxm)! scanning paths for an image of mxm size based on a 2-D spatial accessing method. The high productivity and good security are the most important advantages of SCAN methodology when encoding and decoding images. [19, 21, 22]. Usually, the SCAN language uses four basic scan modes such as continuous orthogonal (O), continuous raster data (R), vortex (S) and continuous diagonal (D). Figure 2. shows a basic scan mode.



(R) Raster (D) Diagonal (O) Orthogonal (S) Spiral

Figure 2. The basic of scan patterns

There are three main sections through which the basic SCAN language is calculated by: (B); (Z); (X) Partition patterns. The basic partition patterns B type, Z type, and the X type shows in Figure 3.



Figure 3. The basic of partition patterns B type, Z type, and the X type

2.4. *The Adjacency and Incidence Matrices in graph theory*

Generally, the graph G is said to be connected if any two vertices in G are connected. Let G be a graph with vertices set and edge set $E(G)= \{e_1, e_2, e_3, \dots, e_m\}$, can be described by means of matrices [17]. The adjacency matrix of is the n-by-n matrix entry is the number of edges in G with endpoints, with rows and columns labelled by vertices. If, then there exists an edge going from vertex to vertex. Likewise, if, then there is no edge from vertex to vertex. Generally, a graph is said to be loopless graph

if it contains no loop. The incidence matrix is the n -by- m matrix in which entry is 1 if q_j incident with and otherwise is 0 [17].

3. The Proposed Algorithm

The fundamental thought of proposed algorithm for encoding the original color image by using a scan pattern as well as block rearranging process. Here, the position of pixels position is changed based on motivated spiral scanning patterns. Our proposed scheme uses the graph theory for generating a voice key.

3.1. An Algorithm for both Scrambling and Encryption

Input: An original color image, speech signal, scan pattern (modified Spirl S)

Output: Cipher color image

A group of steps is:

Step 1: Input the color image of size 256×256 pixels.

Step 2: Read the color image and then split it in to into R, G, and B levels. For each input matrix level (R, G and B), divide the color image into 16 sub-blocks of size 64×64 pixels.

Step 3: Get the starting a modified Spiral S scan to read the values from each sub-block and save them at new block of same size (64×64). Then collect all blocks at new scrambling image of size (64×64). Show Figure 4. and Table 1.

Step 4: Divide each level (R, G and B) into 64 sub-block of length 32×32 pixel at each level do the following steps:

- Convert each block to the vector of length 1024 value.
- Divide the vector into 4 vectors each of which have 256 value.
- Perform XOR operation between the four vectors and secret key vectors. Form the keys matrix selected two keys of length 512 then divide each key into two keys of length 256.
- Perform XOR between the vector and the first part of secret key, the result of this operation has been xored again to the second part of secret key.
- Convert back the four vectors into one vector then convert it back to sub block of 32×32 pixels.
- Use Arnold transform for each sub-block.

Step 5: Combine the 64 sub-blocks back into an encrypted color image of size 256×256 .

Step 6: Store the cipher color image.

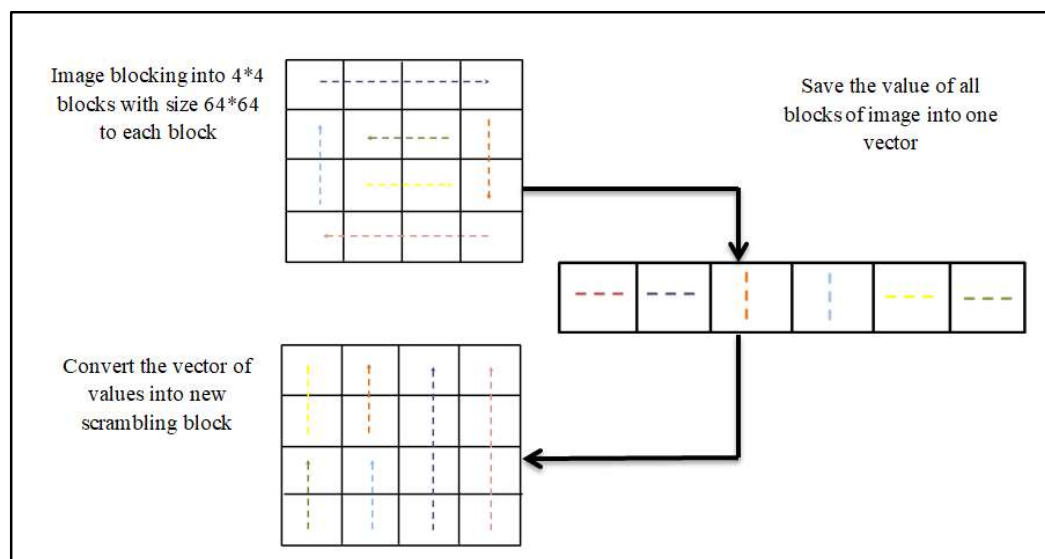








Figure 4. A modified Spiral S scan

Table 1. Modified Spiral S scan

Line Color	Order of reading value from image block	Order of saving value into new image block
	1	6
	2	5
	3	4
	4	3
	5	2
	6	1

3.2. Decryption Algorithm

This section presents the decryption algorithm for proposed image encryption method is described for recovering the original color image from its encrypted version. The following are the sequence of steps used to decrypted images.

Input: Cipher image, described color image

Output: Color image

A group of steps is:

Step 1: Input the cipher color image of sizes 256×256 pixels.

Step 2: Divide each level (R, G and B) into 64 sub-block of length 32×32 pixels at each level do the following steps:

- Use Arnold transform for each sub-block.
- Convert each block to the vector of length 1024 values.
- Divide the vector into 4 vectors each of which have 256 values.
- Perform XOR between the vector and the first part of secret key, the result of this operation has been xored again to the second part of secret key.
- Perform XOR operation between the four vectors and secret key vectors. Form the keys matrix selected two keys of length 512 then divide each key into two keys of length 256.
- Convert back the four vectors into one vector then convert it back to sub block of 32×32 pixels.

Step 3: Combine the 64 sub-blocks back into a decrypted color image of size 256×256 pixels.

Step 4: Read the decrypted color image then divides it in to into R, G, and B levels. For each input matrix level (R, G and B), divide the decrypted color image into 8 sub-blocks of size 64×64 pixels.

Step 5: Get the starting a modified Spiral S scan to return the values from each sub-block to the real position and save them at new block of same size (64×64 pixels). Then collect all blocks at new descrambling image of size (64×64 pixels).

Step 6: Combine the 16 sub-blocks back into a descrambled color image of size 256×256 pixels

Step 7: Store the decrypted color image.

3.3. Key Generation stage

Both of encryption and decryption processes use the same key. The algorithm begins to receive audio signal (verbal) of length 10 ms, which is divided into blocks of size (256) values. Using a graph theory, the blocks convert into square matrices (16×16), where the matrix is defined as a connected graph. The connected graph, in turn, generates the keys by using the adjacency matrix, which works to find the interconnects that denotes by 1 when there is no interconnects denotes by 0. the adjacency matrix was multiplied by the lower triangular matrix $m_{i,j}$, then again $m_{i,j}$ matrix convert to adjacency matrix. Using

the Mod function to reduce the resulting values to be identified between 0-255 (as the pixel values between (0-255)). The Mod function, in turn, generates keys that extract the values as its appear in the matrix (to maintain a randomness) to get a key vector have 512 of length. Figure 5 shows the general encryption algorithm for color image.

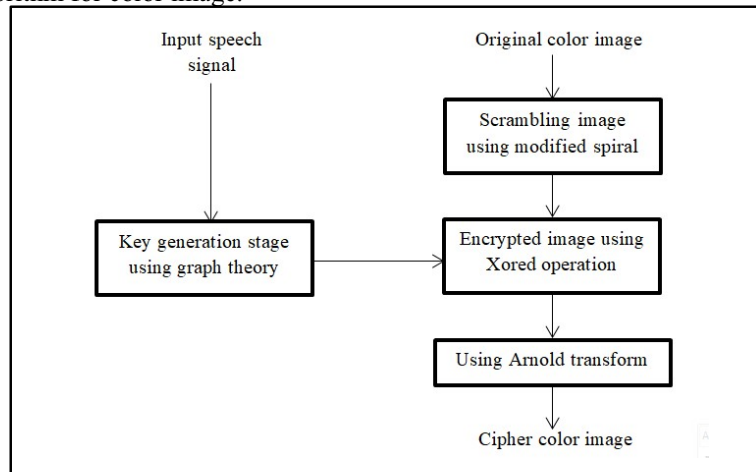


Figure 5. The general encryption algorithm for color image

4. Computation Results

Some of experiments have been implemented by utilizing seven standard color images of size 256×256 pixels (Lena, Pepper, Baboon, Mona Liza, Child, Rose and Barbara), order to verify efficiency of suggested algorithm. Experiments are carried out on MATLAB R2018b software with Windows 10 64-bit, Intel Core i5 Processor. Figure 6 shows the experimental original color image. Efficiency analysis includes six subsections: key space analysis, histogram, entropy, correlation, entropy, differential attack analysis.

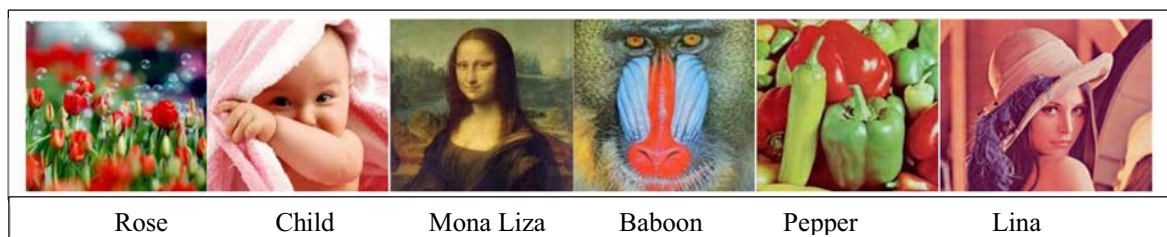


Figure 6. The experimental original color image

4.1. 1. Key Space Analysis

Generally, a key space for encrypting algorithm represents the size of the encryption key. Therefore, the key space should be large enough to ensure resistance to brute force attack. The key space for proposed algorithms depends on four secret keys each of them has $(2)^{256}$.

4.2. Histogram Analysis

An important tool to measure the distribution of pixel weights of the image is a histogram. Usually, the ordinary images have uneven distributions, but the encrypted images have uniform distributions. Thus, uniform histogram is a better to resist the statistic attacks. The histogram results for both original and encrypted images of Lina (256×256 pixels) in three components are show in Figure 7. (a) and 7. (b).



Figure 7 a. The original and encrypted images of Lena

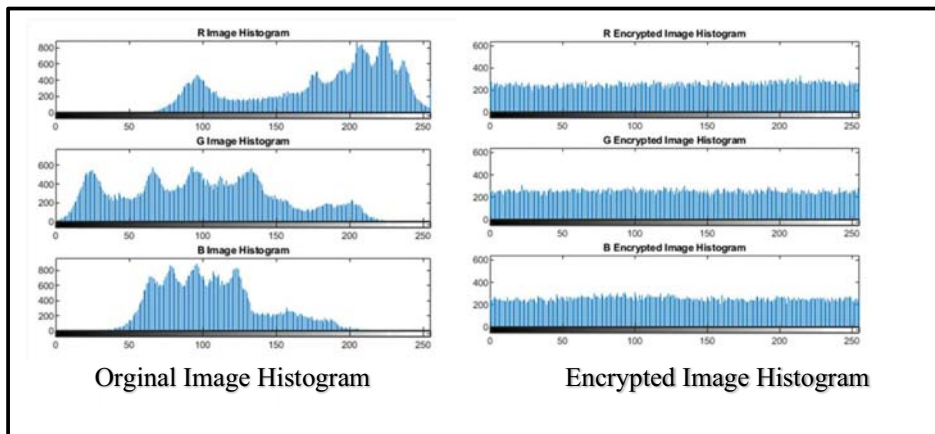


Figure 7 b. The histogram results of the original and encrypted images of Lena

4.3. Entropy Analysis

An entropy is defined as a theoretical tool to measure indeterminateness of image encryption algorithm. It refers the degree of uncertainties and randomness of image pixels. Table 2 shows the entropies of the original color images and its encrypted images. The entropies of the encrypted color images are very close to the theoretical value of 8sh, which indicates that the encrypted image has a capacity against attacks.

Table 2. Entropy Measures of Proposed Algorithm

Color Image	Entropy original image	Entropy encrypted image
Baboon	7.6128	7.9988
Lena	7.7599	7.9987
Pepper	7.7749	7.9987
Mona Liza	7.3808	7.9981

Rose	7.8033	7.9988
Child	7.4639	7.9977
Barbara	7.6454	7.9987

4.4. PSNR and MSE Analysis

The strength of the encrypted image can be analyzed using the Image Quality Assessment (IQA) parameters, such as Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). Usually, PSNR gives an idea about security of encrypted color images by means of its visual quality level. It utilizes to calculate a difference ratio between the original image and an encrypted image according to MSE [23]. The equations for both PSNR and MSE are representing by the following:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

$$MSE = \frac{1}{MN} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} [x(m,n) - \hat{x}(m,n)]^2$$

The results of PSNR and MSE tests are shown in Table 3. The results of a PSNR comparison between the basic image and an image was rebuilt to show these two images are similar.

Table 3. The result for both PSNR and MSE test between a basic image and an image was rebuilt.

Color Image	MSE	PSNR
Baboon	0	INF
Lena	0	INF
Pepper	0	INF
Mona Liza	0	INF
Rose	0	INF
Child	0	INF
Barbara	0	INF

4.5. Correlation Analysis

Correlation analysis is a useful tool that used to measure the similarity between the original image and the encrypted image. The results of correlation coefficients between the original image and the encrypted image are shown in Table 4. Figure 8 shows correlation results on encrypted image.

Table 4. Correlation Coefficients Results

Chosen image	Adjust pixels in correlation analysis	
	Original image	Encrypted image

	Diagonal correlation	Vertical correlation	Horizontal correlation	Diagonal correlation	Vertical correlation	Horizontal correlation
Baboon	0.9437	0.9635	0.9694	0.0048	-0.0013	-0.00033
Lena	0.9212	0.9720	0.9460	-0.0030	0.0006	0.0066
Pepper	0.9478	0.9773	0.9715	0.0009	-0.0046	-0.0010
Mona Liza	0.9866	0.9927	0.9932	0.0065	-0.0030	-0.0095
Rose	0.9636	0.9868	0.9736	-0.0002	-0.0051	-0.0039
Child	0.9567	0.9741	0.9727	0.0026	0.0001	-0.0030
Barbara	0.9040	0.9259	0.8829	0.0021	0.0054	-0.0016

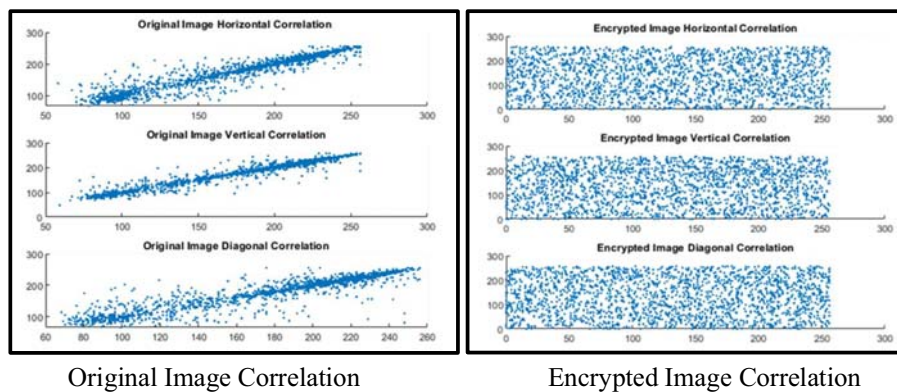


Figure 8. The correlation image before and after encryption

4.6. *Differential Attack Analysis*

The degree of similarity between two different images can be compared using the differential attack Analysis. The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are the two metrics analyze the strength of encryption algorithm. NPCR measures the number of changed pixel rate by changing the one pixel of plain image. UACI is calculated between two encrypted images with change in one pixel in corresponding plain images. Table 5 presents the differential measures of the plain image.

Table 5. The Differential Measures of The Plain Image

Color Image	NPCR	UACI
Baboon	0.9964	0.3065
Lena	0.9959	0.3097
Pepper	0.9959	0.3139
Mona Liza	0.9961	0.3141
Rose	0.9960	0.3277
Child	0.9959	0.3568
Barbara	0.9960	0.3346

The experimental results of proposed algorithm have been compared with those that have been obtained from the similar works in references [24, 25, 26]. The comparisons are made depending on Lena image. The comparisons are made in term of the value of correlation and the results of NPCR and UACI. Tables 6 and 7 below show the comparison of the value of correlation and the results of NPCR and UACI, respectively. The comparison indicates that the correlation value of the proposed algorithm is very close to zero similarly to other work, which makes the proposed algorithm have security against

attacks. Computational results for both NPCR and UACI show that the performance of the suggested algorithm is equal to or better than the schemes in references (22- 24).

Table 6. Comparison of the correlation coefficients

An algorithm	Horizontal Direction	Vertical Direction	Diagonal Direction
Basic Image	0.9460	0.9720	0.9212
Haider & iman	0.0124	-0.00564	0.0276
Paper_87-A	-0.0122	-0.0016	0.0008
Entropy-21	0.0237	0.0237	0.0284
Sci-2019	0.0011	-0.0013	-0.0019
Proposed algorithm	0.0066	0.0006	-0.0030

Table 7. The comparison of results for of NPCR and UACI

An algorithm	NPCR	UACI
Haider & iman	99.63	30.51
Paper_87-A	99.6688	33.6657
Entropy-21	99.6221	33.5887
Sci-2019	99.61	30.41
Proposed algorithm	99.59	30.97

5. Conclusion

In the areas of medicine, military, banking and others, the images are transmitted through open channels that are exposed to potential attacks. Therefore, the exchange of image data requires additional security. For the purpose of securing this channel, this paper presents an encryption algorithm for color images. The suggested algorithm depends on the audio speech files as a basis for exploiting a set of keys for encoding color images. The key generation system was built by passing the audio signal in several stages based on the graph theory. These keys are stored in a database and used to encode the color image by utilizing XOR process. The mathematical results shown that the suggested algorithm has generated the encrypted images with uniform distribution in pixel histograms with information entropy closes to 8, which resists different attacks. The comparison experiments were performed with other recent algorithms. The statistical results show that the proposed algorithm has a strong security against attacks.

References

- [1] Ak, M., Hanoymak, T., & Selçuk, A. A. (2014). IND-CCA secure encryption based on a Zheng-Seberry scheme. *Journal of Computational and Applied Mathematics*, 259, 529-535.
- [2] Storms, J. E. (2016). An evaluation of the history, demand, and current methods for digital steganography (Doctoral dissertation, Utica College).
- [3] Hu, W. T., Li, M. C., Guo, C., & Yuan, L. F. (2015). A Reversible Steganography Scheme of Secret Image Sharing Based on Cellular Automata and Least Significant Bits Construction. *Mathematical Problems in Engineering*, 2015, 1-11. doi:10.1155/2015/849768.
- [4] Zhou, Y. (2008). Multimedia encryption with different security levels using recursive sequences (Doctoral dissertation, Tufts University).
- [5] Bell, R. (2015). Digital steganography: Its impact on mobile forensics, hacking, and social media (Doctoral dissertation, Utica College).

- [6] Villinger, S. (2011, May 9). Crash course: Digital steganography. Retrieved from <http://www.itworld.com/article/2826840/crash-course-digital-steganography.html>.
- [7] Zielińska, E., Mazurczyk, W., & Szczypi, K. (2014). Trends in Steganography. *Communications of the ACM*, 57(3), 86-95. doi:10.1145/2566590.2566610.
- [8] Dominic, B., & Crina, R. (2013). STEGANOGRAPHY AND CRYPTOGRAPHY ON MOBILE PLATFORMS. *Analele Universitatii Maritime Constanta*, 14(20), 121-125.
- [9] Mohapatra, C., & Pandey, M. (2015). A Review on current Methods and application of Digital image Steganography. *International Journal of Multidisciplinary Approach & Studies*, 2(2), 163-178.
- [10] Muhammad, K., Ahmad, J., Sajjad, M., & Zubair, M. (2015). Secure image steganography using cryptography and image transposition. *NED University Journal of Research*, 12(4), 81-91.
- [11] Lou, D. C., Lin, C. L., & Liu, C. L. (2008). Novel steganalysis schemes for BPCS steganography. *Imaging Science Journal*, 56(4), 232-242. doi:10.1179/174313108X283964.
- [12] Ogundele, T. J., & Adetunmbi, A. O. (2014). Evaluation of Multi Level System of Steganography. *International Journal of Information Security Science*, 3(4), 227-231.
- [13] Chang, Y. J., Chen, T. H., & Zhang, W. D. (2010). Biometrics-based cryptographic key generation system and method." U.S. Patent No. 7,804,956. 28 Sep.
- [14] Garcia-Baleon, H. A., & Alarcon-Aquino, V. (2009). Cryptographic key generation from biometric data using wavelets. In *2009 Electronics, Robotics and Automotive Mechanics Conference (CERMA)* (pp. 15-20). IEEE.
- [15] Hao, F., Anderson, R., & Daugman, J. (2005). Combining cryptography with biometrics effectively (No. UCAM-CL-TR-640). University of Cambridge, Computer Laboratory.
- [16] Monroe, F., Reiter, M. K., Li, Q., & Wetzel, S. (2001, May). Cryptographic key generation from voice. In *Proceedings 2001 IEEE Symposium on Security and Privacy*. S&P 2001 (pp. 202-213). IEEE.
- [17] Xu, J. (2003). *Theory and application of graphs* (Vol. 10). Springer Science & Business Media.
- [18] Bourbakis, N. (1986). A Language for Sequential Access of Two-Dimensional Array Elements. *IEEE Workshop on LFA*, pp 52–58, Singapore.
- [19] Berrak, O., Belmeguenai, A., Ouchtati, S. (2019). Secure Transfer of Color Images Using Horizontal and Vertical Scan. *Traitement du Signal*, Vol. 36, No. 1, pp. 45-51.
- [20] Saisubha, V., Priyanka, U., Remya, K. R., Reenu, R. (2013). Image encryption using scan pattern. *Proceedings of AECE-IRAJ International Conference*.
- [21] Adrian, V. D. & Khaled, L. (2013). An Improved Secure Image Encryption Algorithm Based On Rubik's Cube Principle And Digital Chaotic Cipher. *Mathematical Problems in Engineering*, Article ID 848392, vol. 2013, pp. 1-10.
- [22] Monisha, S., Chandrashekhar, K., Amit, G. (2012). A Novel Approach of Image Encryption and Decryption by Using Partition and Scanning Pattern. *International Journal of Engineering Research & Technology (IJERT)* Vol. 1 Issue 7, ISSN: 2278-0181.
- [23] Thakur, N., & Devi, S. (2011). A new method for color image quality assessment. *International Journal of Computer Applications*, 15(2), 10-17.
- [24] Wang, Y., Wong, K. W., Liao, X., & Chen, G. (2011). A new chaos-based fast image encryption algorithm. *Applied soft computing*, 11(1), 514-522.
- [25] Liu, H., & Wang, X. (2012). Image encryption using DNA complementary rule and chaotic maps. *Applied Soft Computing*, 12(5), 1457-1466.
- [26] Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S. (2012). A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Journal of Systems and Software*, 85(2), 290-299.