Hindawi Publishing Corporation
Advances in Multimedia
Volume 2012, Article ID 767364, 8 pages
doi:10.1155/2012/767364

Research Article

Image Encryption Using a Lightweight Stream Encryption Algorithm

Saeed Bahrami and Majid Naderi

Cryptography and Secure Systems Laboratory, Faculty of Electrical Engineering, Iran University of Science and Technology (IUST), Tehran, Iran

Correspondence should be addressed to Saeed Bahrami, bahrami.saeed195@gmail.com

Received 2 November 2011; Revised 21 April 2012; Accepted 23 April 2012

Academic Editor: Mohamed Hamdi

Security of the multimedia data including image and video is one of the basic requirements for the telecommunications and computer networks. In this paper, we consider a simple and lightweight stream encryption algorithm for image encryption, and a series of tests are performed to confirm suitability of the described encryption algorithm. These tests include visual test, histogram analysis, information entropy, encryption quality, correlation analysis, differential analysis, and performance analysis. Based on this analysis, it can be concluded that the present algorithm in comparison to A5/1 and W7 stream ciphers has the same security level, is better in terms of the speed of performance, and is used for real-time applications.

1. Introduction

Nowadays, multimedia data such as image and video is expanding in communications and computer networks [1]. Due to widespread use of multimedia data and despite widespread threats and attacks in communication systems, security of this data is necessary [2, 3]. Multimedia encryption challenges originate from two realities. Firstly, multimedia data have great volumes. Secondly, they need real-time uses [4]. So using encryption for security results in additional computations for information processing. As a result, a balance between security and synchronization requirement is necessary [5]. To reach this aim, we use lightweight and high-speed encryption algorithms. One of the methods to ensure security is considering all data as binary strings and encrypt them using block encryption algorithms such as DES. These algorithms are very complex and involve large amounts of computations, and their software implement is not fast enough for high-volume multimedia data [6].

Commonly stream encryption algorithms are used for image encryption [5, 7–9]. Stream ciphers are built using a pseudorandom key sequence, and then this sequence is combined with the original text through exclusive-or operator. Generally, stream encryption systems have suitable performance when speed and error probability of data transmission are high. In this paper, the simple and lightweight stream encryption algorithm is used for multimedia applications such as image, and also various statistical tests are performed in order to assure the security of the algorithm and compared to A5/1 and W7 stream cipher. The notable point in this algorithm is producing the key sequence by AES block cipher in order to enhance the security.

A5/1 and W7 stream cipher algorithms are used for the key production from the linear feedback shift registers. A5/1 algorithm has 64-bit private key, and W7 algorithm has 128-bit private key. Also, both algorithms have adequate security and proper performance speed for image encrypting as compared to block cipher algorithms such as DES, AES, and RC5. Reference [7] provides more details about these two algorithms and their applications in multimedia security.

This paper is classified as follows. In Section 2, one of the stream encryption algorithms is introduced step by step for multimedia use. Section 3 represents a series of security discussion and statistical tests that include visual test, histogram analysis, information entropy, encryption quality, correlation analysis, differential analysis, and performance

analysis introduced and compared to A5/1 and W7 stream cipher. Section 4 concludes the work results.

2. The Stream Encryption Algorithm

As mentioned in the previous section, stream encryption algorithms are used in attention for real-time applications. In this algorithm, stream ciphers are used in order to accelerate implementation of the algorithm. In order to enhance the security, the key product is the same as the key product of AES block cipher.

In this algorithm, the main text is divided in different sections and each section is encrypted by the stream encryption algorithm. In any section, the encryption algorithm uses a separation secret key. The secret key of our encryption schemes is protected by the block cipher (such as AES). $\mathrm{BE}(m, K)$ denotes a block cipher encryption algorithm on message m using key K, and $\mathrm{SE}(P, \mathrm{key}_i)$ denotes a stream cipher encryption algorithm on message P using key key_i. At the beginning of this algorithm, the key of different sections is generated as $\mathrm{key}_i = \mathrm{BE}(m, K)$, then if the plain text is as $P_1, P_2, \ldots, P_t$, the encrypted text would be as $C_1, C_2, \ldots, C_t$, and any section of the encrypted text is as $C_i = \mathrm{SE}(\mathrm{key}_i, M_i)$.

Let F be a function defined as

$$F\left(\mathrm{Key}_i, X\right) = ((((X \times k_1) \oplus k_2) + k_3) \oplus k_4), \tag{1}$$

where Key_i is the 128-bit key and $\mathrm{Key}_i = k_1 k_2 k_3 k_4$ for 32-bits k_i, x is a 32-bit string, $\oplus$ is the bit-wise exclusive-or, $+$ and $\times$ are mod 2^{32} addition and multiplication. To encrypt every 32 bits of the original text, this algorithm has the following steps.

Step 1. A 128-bit key sequence is generated by the block algorithm AES and is considered to be $\mathrm{Key}_i = k_1 k_2 k_3 k_4$ for 32-bit k_i.

It should be noted that this 128-bit key is updated by the AES algorithm to encrypt every 32-bit of the original text.

Step 2. By the function proposed in (1), A_i value is obtained as follows:

$$A_i = F\left(\mathrm{Key}_i, C_{i-1} \oplus P_{i-1}\right), \tag{2}$$

where X value in (1) is replaced by $C_{i-1} \oplus P_{i-1}$. P_{i-1} and C_{i-1} are equal to 32 bits of the previous plain text and cipher text, respectively. In addition, as it was stated above, $\oplus$ is the bitwise exclusive-or.

Step 3. Again, by the function expressed in (1), B_i value is obtained as

$$B_i = F\left(\mathrm{Key}_i, A_i \oplus P_{i-2}\right). \tag{3}$$

In this step, X value in (1) is replaced by $A_i \oplus P_{i-2}$. P_{i-2} is equal to 32 bits of the original text in the two previous cases, and also A_i was obtained in Step 2 by (2).

Step 4. For the third time, (1) is given as

$$D_i = F\left(\mathrm{Key}_i, B_i \oplus C_{i-2}\right). \tag{4}$$

In this equation, X value in (1) is equal to $B_i \oplus C_{i-2}$. C_{i-2} is equal to 32 bits of the encrypted text in the two previous cases, and B_i was obtained in Step 3 by (3).

Step 5. In this stage, according to the following equation, 32 bits of the cipher text are obtained:

$$C_i = P_i \oplus D_i, \tag{5}$$

where P_i value is equal to 32 bits of the plain text and so D_i value was obtained in Step 4.

All the Steps 2–5 can be summarized by the following equation:

$$C_i = P_i \oplus F\left(\mathrm{key}_i, F\left(\mathrm{key}_i, F\left(\mathrm{key}_i, C_{i-1} \oplus P_{i-1}\right) \oplus P_{i-2}\right) \oplus C_{i-2}\right). \tag{6}$$

In all the Steps 2–4, C_0, C_{-1}, p_0, and p_{-1} can be considered equal to k_1, k_2, k_3, and k_4.

The decryption procedure is similar to the encryption one, just with the difference, the locations of P_i and C_i in (5) are exchanged as follows:

$$P_i = C_i \oplus D_i. \tag{7}$$

It should be mentioned that D_i value in the decryption procedure is obtained in accordance with the encryption procedure as well as using the previous original and encrypted texts.

3. Security and Performance Analysis

The main parameter on design of any encryption algorithm is amount of algorithm robustness against cryptographic attacks including brute force, statistical attack, known plain text attack, and chosen plain text attack. Thus, a cipher of high key and plain text sensitivity is desirable. Besides, computational speed and quality of encrypted images are other important issues. In this section, we performed security discussion of the scheme and a series of tests to compare the efficiency of the described algorithm. Images used to implement the tests are some pictures of USC-SIPI image database (freely available at http://sipi.usc.edu/database/).

3.1. Security Discussion of the Scheme

Security of the Key. The key of the encryption/decryption is Key_i that is produced by the BE block cipher. Therefore, achieving the key is difficult.

Meet in the Middle Attack (the Attack to the Section Key). This type of attack is a brute force attack. By meeting one or more bits in the middle, it searches exhaustively the key bits through the middle bits [5]. Since this algorithm has three rounds of F, the meet in the middle attack does not work. Since at least one way to the middle goes through two rounds of F, therefore, the number of key bits that affects a single bit is large.

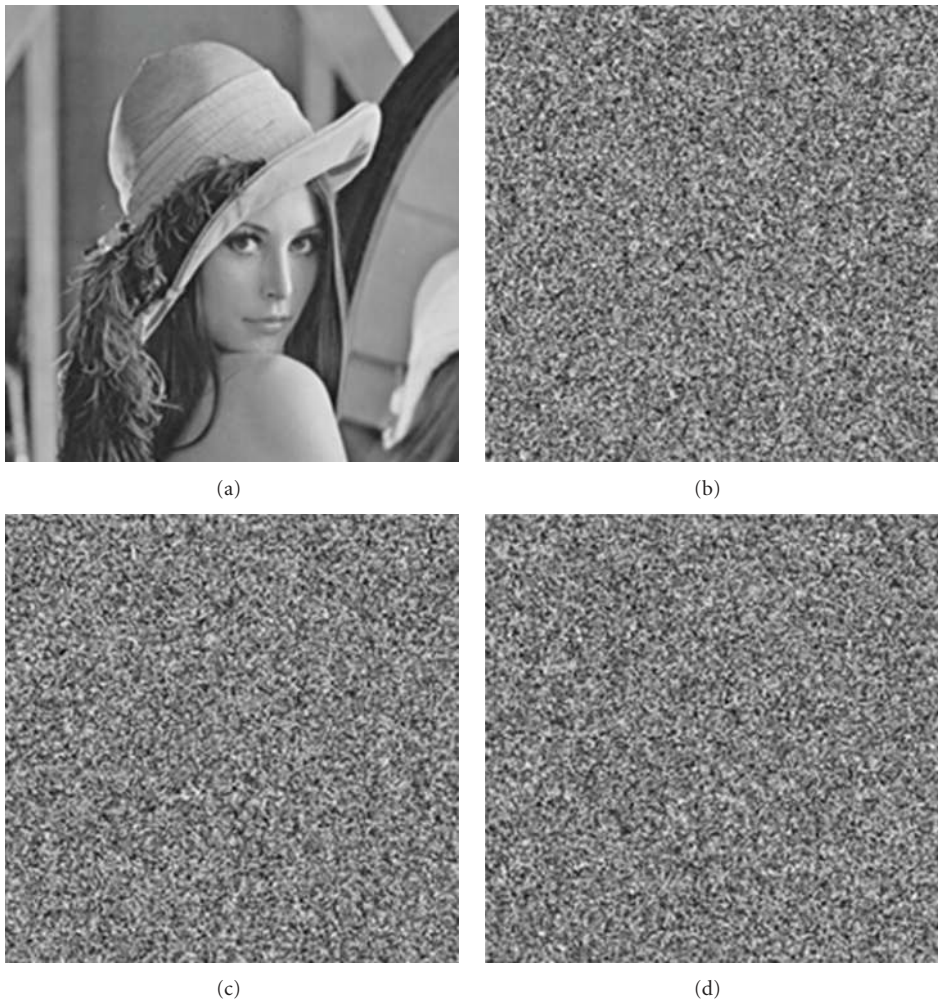

Figure 1: Result of Lena image encryption: (a) the original image, (b) the encrypted image of the described algorithm, (c) the encrypted image of the A5/1 algorithm, (d) the encrypted image of the W7 algorithm.

Chosen Cipher Text Attack (the Attack to the Section Key). All the stream ciphers that have cipher text feedback are weak to the chosen cipher text. For example, if stream cipher was defined as

$$C_i = P_i \oplus F\left(\text{key}_i, F\left(\text{key}_i, F\left(\text{key}_i, C_{i-1}\right) \oplus C_{i-2}\right) \oplus C_{i-3}\right), \tag{8}$$

the cipher would be weak to chose cipher text attack. By choosing $C_{i-3} = C'_{i-3}$, $C_{i-2} = C'_{i-2}$, $C_{i-1} \neq C'_{i-1}$ being different at only one bit, the attacker can ask for the decryption of C_i, C'_i and apply the differential attack [5]. But the stream cipher is defined as

$$C_i = P_i \oplus F\left(\text{key}_i, F\left(\text{key}_i, F\left(\text{key}_i, C_{i-1} \oplus P_{i-1}\right) \oplus b_{i-2}\right) \oplus C_{i-2}\right), \tag{9}$$

where it has both cipher text and plain text feedback. Consequently, achieving the plain text without adequate information from the original text and the encrypted text is impossible.

3.2. Statistical Tests

3.2.1. Visual Test. Observation is an important factor in cipher image test. A good encryption algorithm should mix image so that features are not visually detectable. Also, no information should be observed in the encrypted image by comparing the encrypted and original images [10, 11].

Result of the described algorithm encryption is shown in Figure 1. Figure 1 shows that the encrypted image is quite distinct from the original image.

3.2.2. Histogram Analysis. To prevent the information leakage and aggressive attacks, it must be ensured that the original and encrypted images do not have any statistical similarity. Histogram analysis expresses the way of the distribution of pixels in the image using the drawing number of observations for each amount of pixels brightness [12–16]. Figure 2 shows the histogram analysis on the test image using the described algorithm. The histogram of original image has a sharp rise with a sharp decline as shown in Figure 2(a), and histogram of the encrypted image as shown in Figure 2(b)

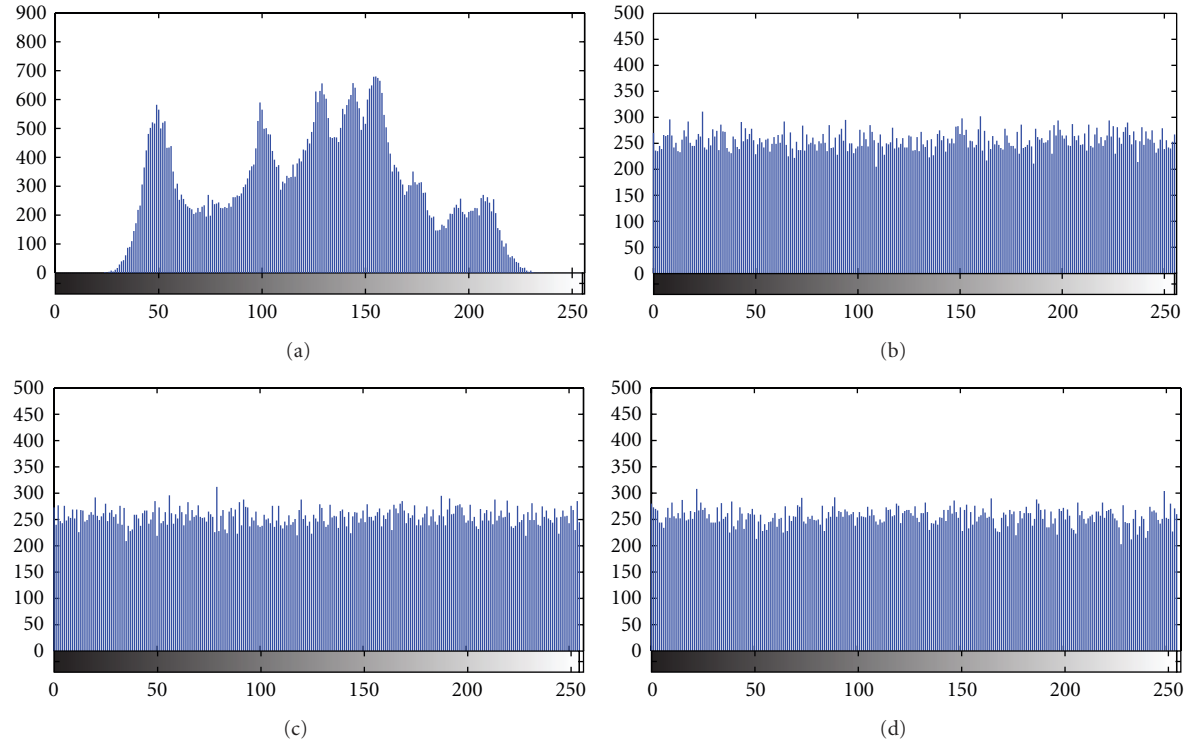

Figure 2: Result of histogram analysis. (a) Histogram of the original image, (b) the described algorithm, (c) A5/1 algorithm, and (d) W7 algorithm.

has a uniform distribution that is completely different from histogram of the original image and has no statistical similarity. Therefore, the attacker with the histogram analysis of the encrypted image cannot acquire information from the original image.

3.2.3. Information Entropy. Shannon introduced information entropy as the measure of source information in 1949. The $H(s)$ entropy of a message source s is defined as

$$H(s) = \sum_{i=0}^{2N-1} P(s_i)\log_2 \frac{1}{P(s_i)}. \quad (10)$$

In this equation, $P(s_i)$ represents the probability of symbol s_i and the entropy is expressed in bits [17]. If we suppose that the source emits 2^8 symbols with equal probability and $s = \{s_1, s_2, \ldots, s_{2^8}\}$, random source entropy is equal to 8. If an encryption algorithm creates symbols with entropy less than 8, there is likelihood to predict original image from encrypted image, which is a threat to the system security. As it is observed in Table 1, entropy of studied algorithms is very close to the ideal value of 8. This means that information leakage in the encryption process is negligible and studied algorithms are secure upon the entropy attack. Also, we conclude that the entropies of A5/1 and the proposed algorithms are closer to the ideal value compared with entropy of W7.

3.2.4. Encryption Quality. The image encryption creates large changes in the amount of pixels. These pixels are completely different from the original image. These changes are irregular. More changes in values of the pixels show more effectiveness of encryption algorithm and thus better quality. Let $C(x, y)$ and $P(x, y)$ be the gray level of the pixels at the xth row and yth column of a $W \times S$ encrypted and original images, respectively. Encryption quality shows the average of changes in each amount of gray L, and, according to [18], it can be expressed as

$$\text{Encryption Quality} = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{256}, \quad (11)$$

where $H_L(P)$ and $H_L(C)$ are the number of repetition from each gray value in the original image and the encrypted

Table 1: Entropy results of encrypted images. Grayscale type with 256×256 size.

File name	File description	The proposed algorithm	A5/1	W7
4.2.04	Girl (Lena)	7.9890	7.9892	7.9886
5.1.12	Clock	7.9899	7.9901	7.9893
5.1.13	Resolution chart	7.9870	7.9890	7.9869
5.1.14	Chemical plant	7.9894	7.9899	7.9894
5.2.08	Couple	7.9884	7.9897	7.9885
5.2.09	Aerial	7.9897	7.9898	7.9897
5.2.10	Stream and bridge	7.9894	7.9896	7.9893
5.3.01	Man	7.9891	7.9899	7.9889
5.3.02	Airport	7.9898	7.9898	7.9899

Table 2: Quality results of encrypted images. Grayscale type with 256×256 size.

File name	File description	The proposed algorithm	A5/1	W7
4.2.04	Girl (Lena)	170	169.38	168.50
5.1.12	Clock	242.80	242.33	241.59
5.1.13	Resolution chart	454.91	455.33	454.61
5.1.14	Chemical plant	206.33	207.10	206.14
5.2.08	Couple	235.55	222.86	220.66
5.2.09	Aerial	265.77	267.99	265.14
5.2.10	Stream and bridge	140.99	141.32	140.84
5.3.01	Man	145.16	145.09	143.71
5.3.02	Airport	288.84	289.16	288.08

image, respectively. Encryption quality for A5/1, W7, and the described algorithm is available for different images in Table 2. From the obtained values, we conclude which the qualities of A5/1 and the proposed algorithm are better than W7.

3.2.5. Correlation Analysis. Any pixel correlates highly with adjacent pixels in the original image. Equations (5), (6), and (7) are used to study the correlation between adjacent pixels in horizontal, vertical, and diagonal orientations [4, 7, 15, 16]:

$$r_{xy} = \frac{\mathrm{Cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_j - \frac{1}{N}\sum_{i=1}^{N}x_j\right)^2, \tag{12}$$

$$\mathrm{Cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_j - \frac{1}{N}\sum_{i=1}^{N}x_j\right)\left(y_j - \frac{1}{N}\sum_{i=1}^{N}y_j\right).$$

In these equations, r_{xy} is correlation coefficient, x and y are intensity values of two adjacent pixels in the image, and N is the number of pair pixels of the selected adjacency in the image to calculate the correlation. 1000 pairs of two adjacent pixels are selected randomly from the image. Ideally, correlation coefficient of the original image is equal to one, and the correlation coefficient of the encrypted image is equal to zero. Also, the correlation diagram is used. Initially, the neighborhood of horizontal, vertical, and diagonal of N pixels is identified in this diagram. Then, diagram is plotted based on the value of each pixel and its neighbors.

As it is specified in Figure 3, correlation between pixels of the original image is too much, while there is a little correlation between neighboring pixels in the encrypted image. In Table 3, correlation coefficients of different encrypted images by studied encryption algorithms have been given for neighborhoods of horizontal, vertical, and diagonal. The table shows that the values of correlation coefficients of the three algorithms are very close to zero for each neighborhood. Therefore, these algorithms are secure against correlation attacks.

3.2.6. Differential Analysis. An encryption algorithm should be designed so that it is sensitive to the small changes in the original image. Attacker tries to view the changes result in the encrypted image making minor changes in the original image. Thus, it reveals a significant relationship between the original image and the encrypted image. Also, this action facilitates finding the algorithm key. If a small change in the original image can cause a large change in the encrypted image, then the differential attack is not possible.

Three common measures were used for differential analysis: MAE, NPCR, and UACI [7, 17]. MAE is mean absolute error. NPCR is the number of pixels change rate of encrypted image, while one pixel of original image is changed.

UACI is the unified average changing intensity, which measures the average intensity of the differences between the original image and the encrypted image.

If $C(x,y)$ and $P(x,y)$ are the gray level of the pixels at the xth row and yth column of a $W \times S$ encrypted and original image, respectively, then MAE is defined as

$$\mathrm{MAE} = \frac{1}{H \times W}\sum_{x=0}^{H-1}\sum_{y=0}^{W-1}|\,C(x,y) - P(x,y)\,|. \tag{13}$$

The MAE test results for the three encryption algorithms have been recorded in Table 4. Information recorded in the table shows that the calculated MAE values of encryption algorithms have little difference.

Consider two encrypted images C_k and $\bar{C}_k$ that, corresponding to original images, are only different in a pixel. The NPCR is defined as

$$\mathrm{NPCR}_k = \frac{\sum_{x=0}^{H-1}\sum_{y=0}^{W-1}D_k(x,y)}{H \times W} \times 100\%,$$
$$D_k(x,y) = \begin{cases} 0, & C_k(x,y) = \bar{C}_k(x,y), \\ 1, & C_k(x,y) \neq \bar{C}_k(x,y), \end{cases} \tag{14}$$

and UACI is defined as

$$\mathrm{UACI}_k = \frac{1}{H \times W} \times \sum_{x=0}^{H-1}\sum_{y=0}^{W-1}\left[\frac{\left|C_k(x,y) - \bar{C}_k(x,y)\right|}{255}\right] \times 100\%. \tag{15}$$

It is clear that large amounts of NPCR and UACI indicate a high sensitivity of the encryption algorithm to the original image. The NPCR and UACI test results have been recorded in Table 5. The results indicate that the NPCR and UACI are less than 0.01% for the studied algorithms. Unfortunately, this means that these algorithms have low sensitivity to changes in the original image.

3.2.7. Performance Analysis. In addition to security issues, the speed of encryption algorithm is important for real-time processing. Efficiency of the proposed encryption algorithm is dependent on the comparison between the speed of encryption algorithms. Efficiency of algorithms has been

Table 3: Correlation coefficient results of encrypted images. Grayscale type with 256 × 256 size.

File name	File description	Neighborhood of horizontal			Neighborhood of vertical			Neighborhood of diagonal		
		The proposed algorithm	A5/1	W7	The proposed algorithm	A5/1	W7	The proposed algorithm	A5/1	W7
4.2.04	Girl (Lena)	−0.0074	−0.0072	−0.0012	0.0072	−0.0522	−0.0122	0.0105	0.0131	0.0017
5.1.12	Clock	0.0320	−0.0130	0.0236	0.0068	−0.0230	0.0220	−0.0840	0.0015	0.0057
5.1.13	Resolution chart	−0.0042	−0.0311	0.0076	0.0196	0.0180	−0.0033	0.0166	−0.0064	0.0196
5.1.14	Chemical plant	−0.0132	0.0177	0.0221	0.0186	−0.0165	0.0364	0.0162	0.0038	−0.0099
5.2.08	Couple	−0.0048	0.0194	0.0227	−0.0149	0.0322	0.0205	0.0149	−0.0052	0.0131
5.2.09	Aerial	0.0094	0.0053	0.0083	−0.0218	0.0098	0.0178	0.0116	−0.0128	0.0184
5.2.10	Stream and bridge	−0.0015	0.0196	0.0017	−0.0357	0.0234	−0.0194	−0.0114	0.0067	−0.0034
5.3.01	Man	−0.0144	0.0084	−0.0402	0.0285	−0.0059	0.0099	−0.0067	0.0085	0.0175
5.3.02	Airport	0.0088	0.0131	0.0166	0.0029	−0.0153	0.0179	0.0196	−0.0223	−0.0182

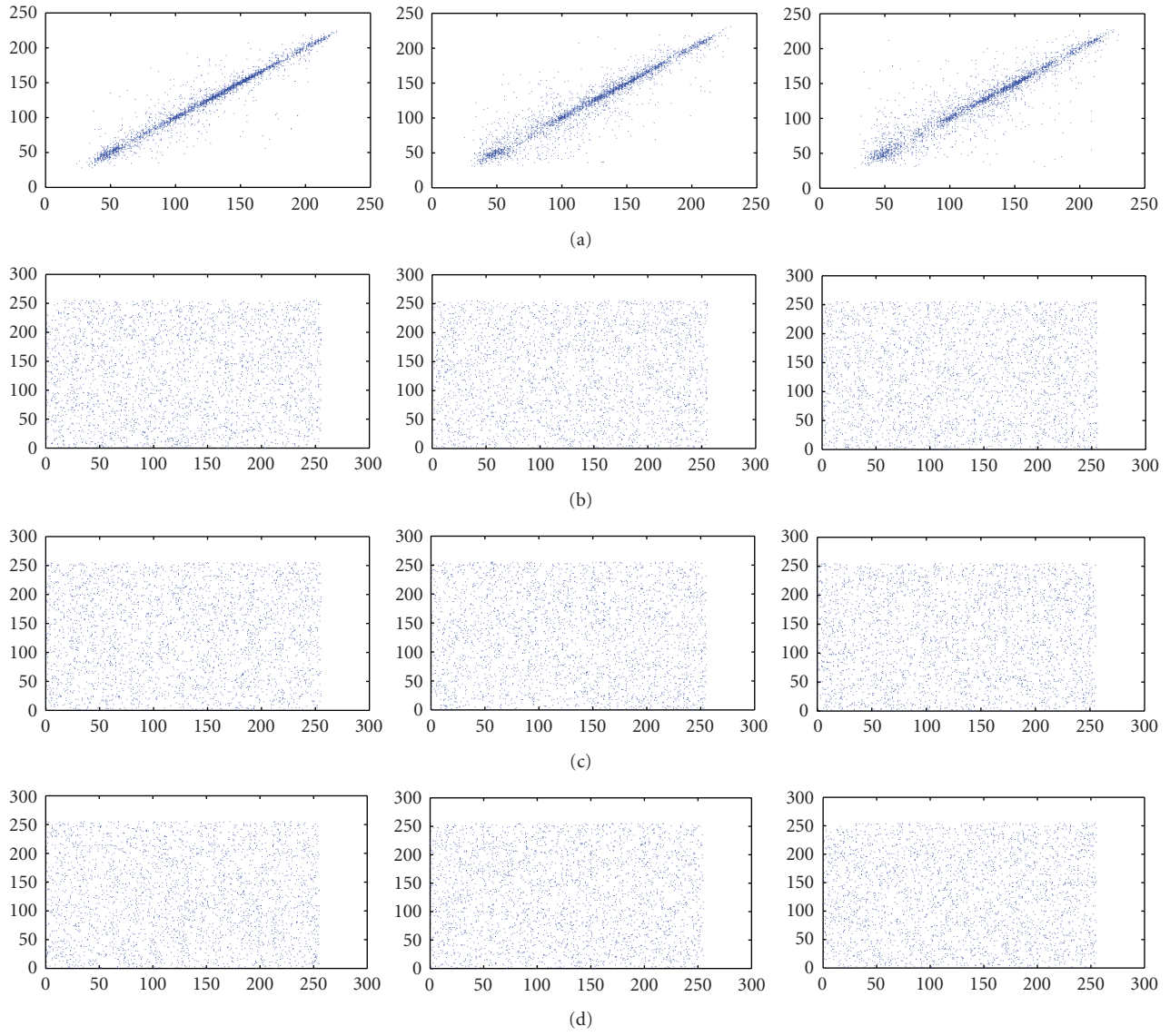

Figure 3: Correlation chart. left side with neighborhood of horizontal, center with neighborhood of vertical, right side with neighborhood of diagonal (a) Lena Standard image (b) the described algorithm (c) A5/1 algorithm and (d) W7 algorithm.

Table 4: MAE test results for Lena standard.

Image size	type	The proposed image	A5/1	W7
256 × 256	grey	72.969	72.706	72.62

Table 5: Compare UACI and NPCR between encryption algorithms in Lena standard image.

Method	NPCR	UACI
The proposed algorithm	%0.0702	%0.0262
A5/1	%0.0015	%0.0005
W7	%0.0015	%0.0006

Table 6: Compare the speed of the studied algorithms in MATLAB programming environment.

Encryption speed comparison (second)			
Size	64 × 64	128 × 128	256 × 256
AES-128	4.23	10.12	65.23
The proposed algorithm	0.191	0.51	1.21
A5/1	0.21	0.87	2.32
W7	0.42	1.01	3.23

achieved with a unoptimized MATLAB code on a machine with Intel core 2 Duo 2.10 processor and 2 Gbytes of RAM memory for Windows 7 operating system. The results in Table 6 show that the described algorithm in terms of execution speed is better than algorithms A5/1 and W7 and so is better for real-time applications.

4. Conclusion

In this investigation, one stream encryption algorithm was proposed for multimedia systems, and many statistical tests were performed to prove suitability of the algorithm, and so this algorithm was compared to A5/1 and W7 stream ciphers. Based on the visual test, there is not any kind of information from the original image in the encrypted image. The histogram shows that distribution of brightness in pixels of the encrypted image is completely uniform, and there is not any statistical similarity with the histogram of the original image. The results of information entropy test show that this value is very close to the ideal value in the encrypted images for all three algorithms. Consequently, these algorithms are secure against entropy attacks. Also, comparison between the entropy of the three algorithms shows that entropies of A5/1 and the proposed algorithms are closer to the ideal value compared with entropy of W7. Based on the results of the encryption quality, the described and A5/1 algorithms have a better quality in the diffusion and confusion of pixels than W7 algorithm. Diagram and coefficients of correlation show that correlation between pixels of the encrypted image has declined severely, and these algorithms are secure against correlation attacks. In order to measure the sensitivity of the algorithm to minor changes in the original image, two measures were considered: NPCR and UACI. The results showed that the proposed algorithm and A5/1 and W7 algorithms have a little sensitivity to minor changes in the original image, ultimately. Performance speed of the described algorithm and two algorithms of A5/1 and W7 were compared. The results showed that performance speed of the described algorithm is faster than two algorithms of A5/1 and W7. According to last discussions, it seems that the described algorithm in software applications has more advantages compared to both algorithms of A5/1 and W7.

References

[1] A. Uhl and A. Pommer, "Application scenarios for the encryption of still visual data," in *Image and video encryption from Digital Rights Management to secured personal communication, Advances in Information Security*, vol. 15, pp. 31–43, Springer, 2005.

[2] S. Lian and X. Chen, "On the design of partial encryption scheme for multimedia content," *Mathematical and Computer Modelling*. In press.

[3] N. Taneja, B. Raman, and I. Gupta, "Combinational domain encryption for still visual data," *Multimedia Tools and Applications*, vol. 59, no. 3, pp. 775–793, 2012.

[4] S. S. Agaian, R. G. R. Rudraraju, and R. C. Cherukuri, "Logical transform based encryption for multimedia systems," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC '10)*, pp. 1953–1957, October 2010.

[5] F. Bao and R. H. Deng, "Light-weight encryption schemes for multimedia data and high-speed networks," in *Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM '07)*, pp. 188–192, November 2007.

[6] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "On the security defects of an image encryption scheme," *Image and Vision Computing*, vol. 27, no. 9, pp. 1371–1381, 2009.

[7] A. Jolfaei and A. Mirghadri, "Survey: image Encryption Using A5/1 and W7," vol. 2, no. 8.

[8] N. Thomas, D. Redmill, and D. Bull, "Secure transcoders for single layer video data," *Signal Processing*, vol. 25, no. 3, pp. 196–207, 2010.

[9] F. Liu and H. Koenig, "A survey of video encryption algorithms," *Computers and Security*, vol. 29, no. 1, pp. 3–15, 2010.

[10] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[11] A. Pande and J. Zambreno, "The secure wavelet transform," *Journal of Real-Time Image Processing*, vol. 18, no. 3, pp. 844–856, 2010.

[12] C. N. Raju, G. Umadevi, K. Srinathan, and C. V. Jawahar, "Fast and secure real-time video encryption," in *Proceedings of the 6th Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP '08)*, pp. 257–264, December 2008.

[13] J. Zhou, Z. Liang, Y. Chen, and O. C. Au, "Security analysis of multimedia encryption schemes based on multiple Huffman table," *IEEE Signal Processing Letters*, vol. 14, no. 3, pp. 201–204, 2007.

[14] W. Li and N. Yu, "A robust chaos-based image encryption scheme," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '09)*, pp. 1034–1037, July 2009.

[15] R. C. Luo, L. Y. Chung, and C. H. Lien, "A novel symmetric cryptography based on the hybrid haar wavelets encoder and chaotic masking scheme," *IEEE Transactions on Industrial Electronics*, vol. 49, no. 4, pp. 933–944, 2002.

[16] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
[17] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.
[18] H. E. D. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," *Optical Engineering*, vol. 45, no. 10, Article ID 107003, 2006.