Chaos-based Cryptography for Color Images

Otilia Cangea
Department of Automatic Control, Computers and Electronics
Petroleum-Gas University of Ploiesti
Ploiesti, Romania
ocangea@upg-ploiesti.ro

Nicolae Paraschiv
Department of Automatic Control, Computers and Electronics
Petroleum-Gas University of Ploiesti
Ploiesti, Romania
nparaschiv@upg-ploiesti.ro

***Abstract*—Data security is one of the most important challenges in the information era; the extended use of big data leads to the necessity of hiding the content of a message from unauthorized users so that, prior to transmission, an encryption has to be performed. Chaotic cryptography, a field of modern cryptology, was recently developed as an application of nonlinear dynamics in the chaotic regime. The paper presents a new approach regarding the implementation of a chaos-based color images encryption algorithm, with a specific application that aims to ensure better information security.**

Keywords—chaos-based encryption algorithm, color image, permutation, diffusion.

I. INTRODUCTION

The requirements regarding secure repository of multimedia transmission are mainly due to sudden recent information technology developments, with proneness to TV channels transmission by Internet that use wireless solutions, as well as to constant improvement of mobile phones capacities [1-4]. At the same time, big developments were achieved in real-time transmission of data derived from diverse automation devices, used in various industrial areas. Today, because of the increase in the size of multimedia data stream, the necessity to compress this type of data in order to store it or send it is vigorously imposing. Various types of more efficient encryption methods take into account the particular characteristics of the signal to eliminate the different gaps that can appear due to the high computational volume requirements of the specific algorithms [5-12].

Encrypting multimedia files aims to transform it so that their content cannot be understood by non-authorized persons. The multimedia signal is regarded as a media stream and, depending on the multimedia information used, algorithms have been developed, implemented on physical or logical level, each having its own encryption power. To this end, one can specify the DES, CBC (Cipher Block Chaining) algorithms used for real-time data transmission, whereas Triple – DES, AES algorithms are used for passive data transmission [13-17].

In order to ensure protection for the video content, traditional cryptography, which is very efficient for information security, has been proven not to be as suitable for at least three important reasons [18].

First, considering the fact that real-time video files have usually large sizes, using traditional cryptography produces significant overload and costs. Secondly, considering digital videos, there is a high data redundancy, as it is highly possible for consecutive frames to be similar, so that the conventional ciphers do not properly highlight all visible information. Moreover, for many video system applications, light encryption would be preferred for preserving some perceptual information, but, unfortunately, this would degrade the data.

Within this context, an increased attention has been devoted to the usage of chaotic theory in implementing the encryption process, in particular for color image encryption [19-20]. The chaotic theory affirms that small variations of certain parameters of a complex system may lead to completely different results, producing the so-called butterfly effect, example deriving from the meteorology area, stating that small weather variations located in a particular area of Earth may lead to significant weather changes in opposite areas.

The founder of this theory is the American mathematician and meteorologist Edward Lorenz, who created models of weather situations and remarked a fundamental characteristic of the chaotic systems: for multiple variations of input values, particular models for final results are favored [21]. Lorenz called these favorite models describing the final status of the system *attractors*. A Lorenz system is a system of ordinary differential equations, having chaotic solutions for certain parameter values and initial conditions; a Lorenz attractor may be defined as a set of chaotic solutions of the Lorenz system.

The main advantage of a chaos-based encryption is the fact that a chaotic signal looks like noise for a non-authorized user and time evolution of the chaotic signal strongly depends on the initial conditions and the control parameters of the generating functions; slight variations result in different time evolutions. Consequently, initial states and control parameters can be efficiently used as keys in an encryption system.

Due to these important benefits, chaos-based video encryption algorithms represent high interest state of the art information technology, with great progress and significant results [6-20]. This paper presents a chaos-based color images encryption algorithm and elaborates a practical specific application that ensures information security.

II. CHAOTIC CRYPTOGRAPHY

Chaos-based encryption algorithms are private keys algorithms that use the same key for both encryption and decryption; based on their property of being sensitive to initial

conditions in order to ensure security, the key is usually elaborated considering the system parameters and its initial conditions.

Related to chaotic characteristics and data security, the basic properties of chaotic systems are [11]:

- Parameters sensitivity: changing a value of system parameters will result in two separate trajectories starting from the same point;
- Ergodicity: the covered trajectory will pass through all points in the distributed phase space;
- Sensitivity to given initial conditions: two trajectories starting from different, but close, points will exponentially separate one from another.

Chaos-based cryptography uses dynamic (chaotic) maps that represent dynamic systems depending upon the initial conditions and data. Any variation, no matter how small, of the initial conditions, will generate a long-term significant deviation of the system history, making any approximation of the result at a specific time almost impossible. Such a dynamic system may have a discrete or a continuous evolution; in the case of a discrete system, a map defines a result as $a_{n+1}=f(a_n)$, that is the value of a_{n+1} state is computed according to a_n previous state, meaning that if initial conditions are known, one can determine the value at a very early stage.

The chaotic state may occur only if the dynamic system is nonlinear and considering particular values associated to the system parameters; one can observe this in the case of a chaotic attractor in the phase space where all evolution trajectories follow a certain pattern, but are never the same [3-5].

Classic encryption algorithms use a combination of confusion and diffusion operations applied in rounds; both operations aim to prevent the deduction of the encryption key. As for chaotic algorithms, encryption is performed in a similar manner, by reiterating the chaotic map, so that it will cover the entire range of stages. A typical structure of chaos-based image encryption scheme is presented in Fig. 1 [19].

Up to the present, most of chaos-based encryption algorithms were implemented within analog transmission systems; the reason why implementation within digital systems generates problems is related to the fact that these systems use devices that allow only a finite number of spaces, thus limiting the possible initial state due to the property of sensitivity associated to parameters and conditions.

For analog data transmission, the encryption system needs a synchronization between the two entities that communicate. Information can be transferred using different methods: *chaotic masking*, when the message is added at the output of a chaotic generator using a transmitter, *chaotic exchange,* when a binary message is used for choosing the signal carrier from between many chaotic attractors, and *chaotic control,* when tiny perturbations are added to obtain dynamic symbols of the chaotic system that have to correspond to a symbol sequence. The signal receiver must synchronize with the chaotic generator of the transmitter in order to be able to retrieve the chaotic carrier signal. For digital data transmission, security is ensured by using chaotic maps for message encryption.

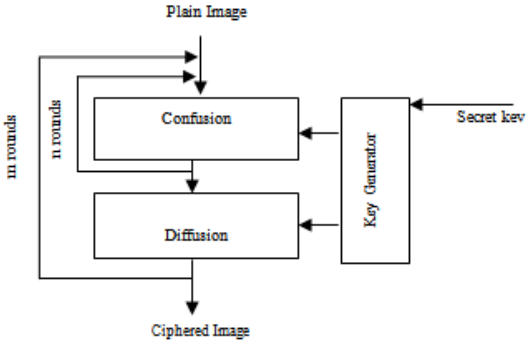


Fig.1. Typical architecture of a chaos-based image encryption scheme

There are various methods used for performing this, among these being the following:

- using ciphers based on pseudo-random number generation [22]; unforseeable pseudo-random trajectories can be thus generated, most of the algorithms are based on this method, using then the resulted values for the encryption/decryption keys;
- using block ciphers based on chaotic feedforward-feedback iterations [23]; these are based on 2D chaotic maps applied in iterations on plain image pixels pseudo-random permutted, followed by a substitution method that equalizes image histogram, repeated in rounds, in order to obtain the encrypted image;
- using block cyphers based on S-type round functions (S-boxes) [24]; this is one of the best methods, as it allows to draw a parallel among classical encryption methods.

These methods do not need synchronization and use chaotic maps, control parameters and initial conditions in order to generate the encryption/decryption keys.

III. Chaos- based Encryption Algorithm for Color Images

The developed chaos-based encryption method that is presented in this paper allows color images encryption by simultaneously encrypting the R, G, and B components of a color image. Up to the present, the other encryption methods mostly used the same principle for R, G, B encryption, that is an independent three-times encryption of the image, without considering the correlation between these components, and thus resulting in a high vulnerability to cyber attacks.

In order to solve this problem, the authors use a chaotic system for encrypting R, G, B one at a time. By combining the strategies of permutation and diffusion, the correlation between components is thus considered, and the encryption performance is increased.

Hereinafter, the specific encryption/decryption stages are presented.

1. It is considered that the dimension of a P plain color image is M*N, M=number of rows, N=number of columns;

2. P image is converted into R, G, and B components; each of these, representing a color, is a M*N matrix, with pixel values in the range 0-255;
3. The logistic map used in this chaotic system has the form:

$$x_{n+1}=ax_n(1-x_n) \quad (1)$$

$x_n \in (0,1)$, a values in the range (3.5699456,4).

4. Permutation stage, performed in two steps.

A. Repeatedly mixing rows
   A.1. Initial values for a and for x_0 are set, then a reiteration is performed for $m+3M$ times and the first m values are eliminated to avoid side effects;
   A.2. $3M$ $\{x_{m+1},x_{m+2},...,x_{m+3M}\}$ values are sorted, leading to $\{x`_{m+1},x`_{m+2},...x`_{m+3M}\}$;
   A.3. Position of $\{x`_{m+1},x`_{m+2},...,x`_{m+3M}\}$ values in $\{x_{m+1},x_{m+2},...,x_{m+3M}\}$ are determined and are marked in TM=$\{t_1,t_2,...,t_{3M}\}$;
   A.4. R, G, B matrices are vertically combined, P1 matrix ($3M$ rows and N columns) is generated;
   A.5. P1 rows are rearranged, corresponding to the positions in TM, so that t_1 row will be placed in the first position, t_2 row at the second position, and so forth, until all rows have been displaced. At the end of this stage, the transformed matrix P_{11} is generated.

B. Repeatedly mixing columns
   B.1. Intial values for a_1 and for y_0 are set, then a reiteration is performed for the chaotic system for $n+3MN$ times, eliminating the first value n to avoid side effects, the chaotic sequence y_n being obtained, (n=1,2,3,...,$3MN$);
   B.2. y_n is divided into M chaotic sequences $y_i=\{y_{i1}, y_{i2},..., y_{i(3N)}\}$ (i=1,2,3,...,M), each sequence having $3N$ values;
   B.3. y_i is sorted, as previously presented, TN_i positions being obtained, $TN_i=\{p_{i1},p_{i2},...,p_{i(3N)}\}$ (i=1,2,3,...,M);
   B.4. P_{11} matrix is divided into three matrices, R_1, G_1, and B_1, each of $M*N$ size, from up to bottom;
   B.5. R_1, G_1, and B_1 are horizontally combined, resulting P_2 matrix, $M*3N$ size;
   B.6. P_2 columns are rearranged, corresponding to TN_i, so that the element from p_{i1} column of the i row is displaced on the first column, then p_{i2} column of i row is displaced on the second column, and so forth, until all columns have been displaced. The transformed P_{22} matrix is thus generated.

5. Diffusion stage
   1. Using y_n, n=1,2,...,$3MN$, the following calculations will be performed:

$$Z_{1n}=mod(y_n*10^{14},3) \quad (2)$$

$$Z_{2n}=mod(y_n*10^{14},256) \quad (3)$$

   2. P_{22} is divided into three matrices, R_2, G_2, and B_2, from left to right, each of $M*N$ size;
   3. R_2, G_2, and B_2 will be converted into R_i^p, G_i^p, B_i^p (i=1,2,...,L) arrays, $L=M*N$;
   4. z_{1n} is used as a reference, that is if z_{1n}=0, then R_i^p current value will be diffused, until all R_i^p current values were diffused; if z_{1n}=1, G_i^p all current values will be diffused, and, similar, for z_{1n}=2, B_i^p all current values;
   5. Diffusion process is performed according to the equation: $C_{current}=(P_{current}+z_{2n}+C_{antecedent}+P_{antecedent})$ mod 256, with $C_{current}$ as encrypted current value, $P_{current}$ as plain image current value, $C_{antecedent}$ as encrypted previous value and $P_{antecedent}$ as plain image previous value. P_0 and C_0 are set as P_0=0, C_0=0;.
   6. After diffusion, three encrypted arrays will result, namely R_i^c, G_i^c, B_i^c (i=1,2,...,L);
   7. The above obtained arrays are converted into three $M*N$ matrices, each of these representing the encrypted R, G, B components of the image;
   8. The last stage is represented by the combination of the three components in a single image, thus resulting the encrypted image.

The decryption process follows the same stages as the encryption process, but in reverse, that is :

1. Initial parameters and values are set identically to those specific to encryption;
2. TM and TN_i , y_i positions are determined;
3. z_{1n}, z_{2n} are computed;
4. The encrypted image is converted into the R, G, and B components, then into the R_i^c, G_i^c, B_i^c arrays, (i=1,2,...,L), with $L=M*N$;
5. Diffusion process is performed according to the equation: $P_{current}=(C_{current}-z_{2n}-C_{antecedent}-P_{antecedent})$ mod 256 , with z_{1n} as reference, $C_{current}$ as encrypted current value, $P_{current}$ as decrypted current value, $C_{antecedent}$ as encrypted previous value and $P_{antecedent}$ as decrypted previous value; first step is set with P_0=0, C_0=0;
6. Consequently to the inverse diffusion stage, R_i^p, G_i^p, B_i^p arrays are obtained, (i=1,2,...,L);
7. All three arrays are converted into matrices, each having $M*N$ size, thus resulting R_2, G_2, and B_2 matrices;
8. The three matrices are horizontally rearranged, resulting P_{22} matrix, with M rows and $3N$ columns;
9. Inverse permutation is performed for the columns of each row for P_{22}, according to TN_i and the P_2 matrix is obtained;
10. P_2 is divided into three $M*N$ size matrices R_1, G_1, and B_1 from left to right;
11. R_1, G_1, and B_1 matrices are vertically rearranged and P_{11} matrix is obtained, with $3M$ rows and N columns;
12. Inverse permutation is performed for P_{11}, according to TM and the P_1 matrix results;
13. P1 matrix is divided into three matrices, each resulted part, namely R matrix, G matrix, and B matrix, being

of *M*N* size and representing the components of the encrypted color image. Using these, one can retrace the initial plain image.

IV. Chaos- based Encryption Application

The chaos-based encryption video files application was performed following the stages presented below.

1. In order to implement the chaos-based encryption algorithm previously presented, a video file with *mp4, avc, avi* or *wmv* extensions is needed; for example, this can be selected using the corresponding push button of the Java implemented graphical interface, presented in Fig. 2.
2. The selected video file is then divided in two parts. The first part will contain all the frames with the file images, obtained by reading the file data and saving the current frame so that thirty frames will be saved for each second of the video file.

Fig.2. Graphical interface for the encryption application

The second part will read the bit stream associated to the audio channel, then this stream will be saved into an encoder container, consequently used for creating a new file (only audio-type, in this case). For each of these two parts, the chaos-based encryption/decryption specific algorithms can be implemented .

3. Hereinafter, the results for the encryption-decryption algorithm for the original test image in Fig. 3. will be presented.

Fig.3. Original test image

The test image in Fig. 3. is a color image, so it complies with the first condition of the algorithm. The R (red) matrix, G (green) matrix, and B (blue) matrix from the original image will be extracted, in the form presented in Fig. 4 a), b), respectively c).

a)

b)

c)

Fig. 4. Extracted images a) R ; b) G; c) B

Firstly, one will form a new image that contains all three components R, G, and B vertically superimposed, as seen in Fig. 5.

Fig. 5. Image obtained after superimposing R, G, and B components

As a result of vertically rearranging rows depending on the sorted positions of TM, the image in Fig. 6. is displayed.

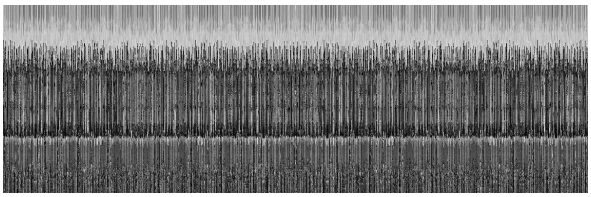
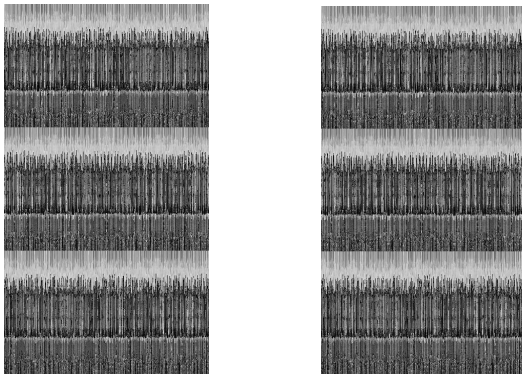


Fig. 6. Image obtained after vertically rearranging rows

After that, one can obtain a new image by adding R, G, and B components values horizontally reunited, as in Fig. 7.a, and another image as a result of rearranging the columns considering the values contained in TN_i, that represent the positions, as in Fig. 7.b.

It is very important to emphasize the fact that the values used for initial parameters and conditions are a=3.7; a_0=3.9; x_0=0.6, and y_0= 0.7 .

After all these operations have been completed, the effective encryption is implemented, using z_{1n} and z_{2n} values and the diffusion function, for each pixel of the image. The resulted encrypted image is presented in Fig. 8. It is obvious that the encrypted image does not contain any clear form, being a random mix of colors.



a) b)

Fig. 7. Image obtained after R,G, B components are added together horizontally (a) and after horizontally rearrranging columns (b)

For decryption, the same operations are performed, but in the reverse order. It is important to emphasize the fact that the same values for initial conditions and parameters have to be used. Contrariwise, the image would not be accurately decrypted; so, for a=3.6, a_0=3.9, x_0=0.6, and y_0=0.7, the image has the form presented in Fig. 9.

Fig. 8. Encrypted image

If correct values are used, the image will be accurately decrypted with R, G, B components as seen in Fig. 10 a), b), respectively c).

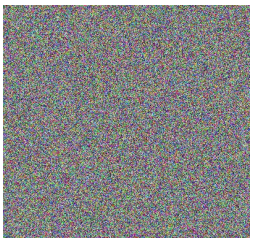


Fig. 9. Decrypted image with wrong values as initial conditions

a)

b)

c)

Fig. 10. Results for accurate image decryption: a) R; b) G; c) B.

Each of these images, containing only R, G, and B values, are then appropriately associated, having as a result the final decrypted image presented in Fig. 11.

Fig. 11. Final form of accurately decrypted image

V. CONCLUSION

The studied chaos-based encryption algorithm presents a high sensitivity to the values of the initial conditions, any tiny variation of these leading to different results, so that they are very difficult to be obtained using various cyber attack methods.

This encryption algorithm was chosen after testing several different methods based on the same chaotic principle, but that have proved to be much too slow, due either to the big computational volume, or to the requirement to save permutation tables needed for the decryption phase that, furthermore, represents a great vulnerability.

Future research directions will have to consider implementation of the same encryption/decryption algorithm for the audio section, as well as elaboration of functions that allow the restoration of the initial video file by methods of reconstruction the visual section by reuniting all saved image frames having the same properties as the initial file.

REFERENCES

[1] J. Shah and V. Saxena, "Video Encryption: A Survey", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, pp.525-534, March 2011.

[2] A. Pande and J. Zambreno, " Embedded Multimedia Security Systems. Algorithms and Architectures", Chapter 2, pp.22-30, Springer, 2013.

[3] L. Kocarev, "Chaos-Based Cryptography: A Brief Overview", IEEE Circuits and Systems Magazine , vol. 1, issue 3, pp. 6-21, Third Quarter 2001.

[4] S. P. Singh, D. Jha, S.Singh, "Generation of Image Encryption Key on the basis of Chaos and Strange Attractors", Proceedings of the International Conference on Advances in Electronics, Electrical and Computer Science Engineering — EEC 2012, pp.425-428, 7-9 July 2012, Dehradun, India.

[5] G. Makris and I. Antoniou, "Cryptography with Chaos", Proceedings of the 5th Chaotic Modeling and Simulation International Conference, Aristotle University, Thessaloniki, Greece, pp.169-178, 12 – 15 June 2012.

[6] W. Xingyuan and L. Teng, X. Qin, "A novel colour image encryption algorithm based on chaos", Journal of Signal Processing, vol.92, issue4,April,2012, pp. 1101-1108, Elsevier North-Holland, 2012.

[7] S. Singh, N. Verma, V. Kumar, "A Survey Report on Video Encryption and Decryption Techniques", International Journal of Computer Science and Mobile Computing, vol.3, issue 12, pp.270-274, December 2014.

[8] L.Tang, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", in MULTIMEDIA' 96 Proceedings of the fourth ACM International Conference on Multimedia, pp. 219-229,1996.

[9] C. Shi and B. Bhargava, "Light Weight MPEG video Encryption Algorithm", in Proceeding of the International Conference on Multimedia, January 23-25, pp. 55-61, New Delhi, India, IETE, Tata McGraw-Hill Publishing Company, 1998.

[10] D. Socek, H. Kalva, S. S. Magliveras, O. Marques, D.Culibrk, and B. Furht, "A Permutation-based Correlation-Preserving Encryption Method for Digital Videos", International Conference on Image Analysis and Recognition ICIAR 2006, pp. 547-558, 2006.

[11] G.A. Spanos and T.B.Maples, " Performance Study of a Selective Encryption Scheme for the Security of Networked, Real Time Video", Proceedings of the International Conference on Computer Communications and Networks, IEEExplore Digital Library, pp.2-10,1995.

[12] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm", MULTIMEDIA' 98 Proceedings of the 6th ACM International Conference on Multimedia, pp. 81-88, Bristol, United Kingdom, September 13-16, 1998.

[13] C. Shi, S. Y.Wang, B. Bhargava, "MPEG Video Encryption in Real-time using Secret Key Cryptography", Proceedings of the International Conference on Parallel and Distributed Processing Algorithms and Applications, pp. 191-201, Las Vegas,1999.

[14] J. Wen, M. Severa, W. Zeng, M. H. Luttrell, W. Jin, "A Format-Compliant Configurable Encryption Framework for Access Control of Video", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 12, No. 6, pp. 545-557, 2002.

[15] M. Pazarci and V. Dipcin, "A MPEG2-Transparent Scrambling Technique", IEEE Transactions on Consumer Electronics, Vol. 48, No. 2, pp. 345-355, May 2002.

[16] S. Li, G. Chen, A. Cheung, B. Bhargava, K.T. Lo, "On the Design of Perceptual MPEG Video Encryption Algorithm", IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, No. 2, pp. 366-375, 2007.

[17] E. Yavuz, R. Yazici, M. C. Kasapbaşi, E. Yamaç, "A Chaos-based Image Encryption Algorithm with simple logical Functions", Computers & Electrical Engineering, vol.54, August 2016, pp. 471-483, Elsevier ltd, 2016.

[18] Su Z., Lian S., Zhang G., Jiang J. (2011) "Chaos-based Video Encryption Algorithms". In: Kocarev L., Lian S. (eds) Chaos-Based Cryptography. Studies in Computational Intelligence, vol 354, pp.205-226, Springer, Berlin, Heidelberg, 2011.

[19] Lian, S., Sun, J., Wang, Z., "Security Analysis of a Chaos-based Image Encryption Algorithm", Physica A 2005; 351:645-61, 2005.

[20] N.A. Al-Romema, A.S.Mashat, I. AlBidewi, "New Chaos-Based Image Encryption Scheme for RGB Components of Color Image", Computer Science and Engineering, 2012, pp. 77-85, Scientific & Academic Publishing Co., CA, USA.

[21] E. Lorenz, "Deterministic Nonperiodic Flow", Journal of the Atmospheric Sciences, vol. 20, pp. 130-141, 1963.

[22] M. Mishra and V.H. Mankar, "Text Encryption Algorithms based on PseudoRandom Number Generator", International Journal of Computer Applications (0975-8887), vol. 111 – No 2, pp. 1-6, February 2015.

[23] Q. Zheng, X. Wang, M. Khurram Khan, W. Zhang, B.B. Gupa, W. Guo, "A Lightweight Authenticated Encryption Scheme Based on Chaotic SCML for Railway Cloud Service", In special section on Recent Advances in Computational Intelligence Paradigms, for Security and Privacy for Fog and Mobile Edge Computing, vol. 6, pp. 711-722, 2018.

[24] T.T. Kim Hue, T.M.Hoang, D. Tran, "Chaos-based S-box for Lighweight Block Cipher", IEEE Research Gate October 2014, DOI: 10.1109/CCE.2014.6916765, pp. 572-577, 2014.