ISSN:0975-9646
G.Madhuri et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (6) , 2016, 2476-2480

Chaotic Maps for Key Generation in Block Cipher for Multimedia Encryption/Decryption

G.Madhuri, (M.Tech),
Student,
Department of CSE,
PVPSIT, Kanuru, India

I.M.V.Krishna, M.Tech,
Assistant professor,
Department of CSE,
PVPSIT, Kanuru,India

Abstract: Multimedia data is vastly increasing day by day due to social media and other applications. The reason behind this data growth is increasing number of devices to internet is also increasing. So the security becomes bottle neck while data travelling in the network. Data encryption algorithms are emerged to protect the data while data travelling from one node to another node through network. To carry out such privacy and security for multimedia data like images and videos encryption techniques are using. To protect the multimedia data content over the network there are some technical issues. This paper explains different vulnerabilities of threats for data and encryption algorithms to secure the data through network.

INTRODUCTION

The emergence of Multimedia technology has promoted images and videos to play a more momentous role than the traditional algorithms which demands a serious safeguard of users' privacy. To carry out such security and privacy needs in various multimedia applications, encryption of images and videos is very important to defend our data from malicious attacks of unauthorized parties. Many control mechanisms for authentication purpose can be used to secure distributed multimedia data. But with the rapid growth in the use of digital multimedia data by various digital processing applications and worldwide accessibility of multimedia data in the internet has created threat for the multimedia data. Another major challenge is to protect the multimedia content over the network by dealing with the technical challenges on the characteristics of multimedia content.

LITERATURE REVIEW

Saurabh Sharma, Pushpendra Kumar Pateriya, Lakshmi, et al, illustrates "increasing public concern these days, encryption is becoming popular for communication any type of sensitive data. With the increase in the development of multimedia technologies, the multimedia data are transmitted in the various fields like commercial, medical and military fields, which generally include some sensitive data. Here are lots of encryption algorithms proposed for the video transmission. In this paper, classifications well as the description of various video encryption algorithms are presented. The analysis is with respect o some parameters like encryption speed, security level and stream size. It is difficult for a particular algorithm to satisfy all performance parameters. So, encryption algorithm can be selected depending upon requirements of application in use".

Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas, Aniket More, et al, illustrated "Securing multimedia data has become of utmost importance especially in the applications elated to military purposes. With the rise in development in computer and internet technology, multimedia at has become the most convenient method for military training. An innovative encryption algorithm for videos compressed using H.264 was proposed to safely exchange highly confidential videos. To maintain a balance between security and computational time, the proposed algorithm shuffles the video frames along with the audio, and then AES is used to selectively encrypt the sensitive video codewords. Using this approach unauthorized viewing of the video file can be prevented and hence this algorithm provides a high level of ecurity. A comparative study of the proposed algorithm with other existing algorithms has been put forward in this paper to prove the effectiveness of the proposed algorithm".

Michael François, Thomas Grosges, Dominique Barchiesi, Robert Erra, et al, The paper describes "a symmetric encryption algorithm based on bit permutations and using an iterative process combined with a chaotic function. The main advantages of such a cryptosystem are its ability to encrypt securely bit sequences and assuring confusion, diffusion and in distinguish ability properties in the cipher. The algorithm is applied on the image encryption where the plain-image is viewed as binary sequence. The results of statistical analysis about randomness, sensitivity and correlation on the cipher-images show the relevance of the proposed cryptosystem".

Ephin M, Judy Ann Joy, N. A. Vasanthi, et al, says that "Nowadays security becomes an important issue of communication and storage of images. One of the method used to ensure the high security of images is encryption. Images are used in many fields such as biometric authentication, medical science, military; they are stored or transferred through the network and the security of such image data is important. Due to some intrinsic features of the images, such as bulk data capacity and high correlation among pixels the earlier encryption techniques such as AES, DES, RSA, etc are not suitable for practical applications. The attest trend in encryption is chaos based. It has many unique characteristics such as the sensitive dependence on initial conditions, non-periodicity, non-convergence, and control parameters. In this paper survey of different chaos-based image encryption techniques has been discussed".

K. Sakthidasan and B. V. Santhosh Krishna, et al, explained that "recent researches of image encryption algorithms have been increasingly based on chaotic systems, but the drawbacks of small key space and weak security in one-dimensional chaotic cryptosystems are obvious. This paper, a new image encryption scheme which employs one of the three dynamic chaotic systems (Lorenz or Chen or LUchaotic system selected based on 16-byte key) to shuffle the position of the image pixels (pixel position permutation) and uses another one of the same three chaotic maps to confuse the relationship between the cipher image and the plain-image (pixel value diffusion), thereby significantly increasing the resistance to attacks. The proposed system has the advantage of bigger key space; smaller iteration times and high security analysis such as key space analysis, statistical analysis and sensitivity analysis were carried out. The results demonstrate that the proposed system is highly efficient and a robust system".

G.A.Sathishkumar, Dr. Bhoopathy bagan K, et al, illustrated that "In the recent world, security is a prime important issue, and encryption is one of the best alternative way to ensure security. Moreover, here are many image encryption schemes have been proposed, each one of them has its own strength and weakness. This paper presents a new algorithm for the image encryption/decryption scheme. This paper is devoted to provide a secured image encryption technique using multiple chaotic based circular mapping. In this paper, first, a pair of sub keys is given by using chaotic logistic maps. Second, the image is encrypted using logistic map sub key and in its transformation leads to diffusion process. Third, sub keys are generated by four different chaotic maps. Based on the initial conditions, each map may produce various random numbers from various orbits of the maps. Among those random numbers, a particular number and from a particular orbit are selected as a key for the encryption algorithm. Based on the key, a binary sequence is generated to control the encryption algorithm. The input image of 2-D is transformed into a 1- D array by using two different scanning pattern (raster and Zigzag) and then divided into various sub blocks. Then the position permutation and value permutation is applied to each binary matrix based on multiple chaos maps. Finally the receiver uses the same sub keys to decrypt the encrypted images. The salient features of the proposed image encryption method are loss-less, good peak signal –to noise ratio (PSNR), Symmetric key encryption, less cross correlation, very large number of secret keys, and key-dependent pixel value replacement".

RELATED WORK

In this section, the front end design and the user interfaces of the developed system has been made familiar to the user through the set of screenshots of the sequence of processes that are in the system. These screenshots introduce the environment to the end user and explain how the user has to work with the system.

Login page and validation of sender:

The sender First Logs into the system with his Login credentials and is authenticated to enter into the system. If the Login succeeds, the user is directed to the further processing in the system. This is shown in Fig.1.

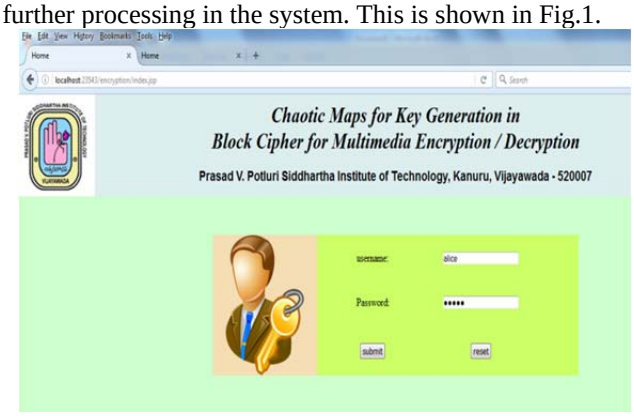

Fig.1. Sender Login page

Login page and validation of receiver:

The receiver First Logs into the system with his Login credentials and is authenticated to enter into the system. If the Login succeeds, the user is directed to the further processing in the system. This is shown in Fig.2.

Fig.2. Receiver login page

Upload Option:

If the user wishes to process with a new image, he can click upload new link, and is directed to an option menu, where he/she can select an image to upload from his computer. After the upload completes, the user is directed to the home page again. This is shown in Fig.3, Fig.4 and Fig.5

Fig.3. Uploading Image in sender

Fig.4: At the upload menu the user can select an image from his/her computer and save it to the image database.

Fig.5. after the upload completes, the user is redirected to the home menu again

Encryption and Sending:

After the image is selected, the user can perform encryption on the image by clicking the button below the image details. The image is inputted to the encryption system which produces a cipher image using the proposed key generation algorithm with a simple encryption technique. And the result is displayed as a message to the user and the option to send the encrypted image is shown to the user. When the user hits the button, the encrypted image is sent as packets over the network to the receiver node and the completion of the encryption phase commences with a success message to the user. This is shown in Fig.6

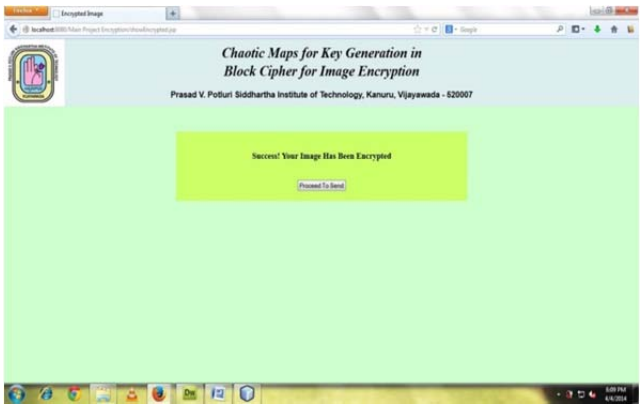

Fig.6: When User hits the button, the image is encrypted and a relevant message is displayed to the user

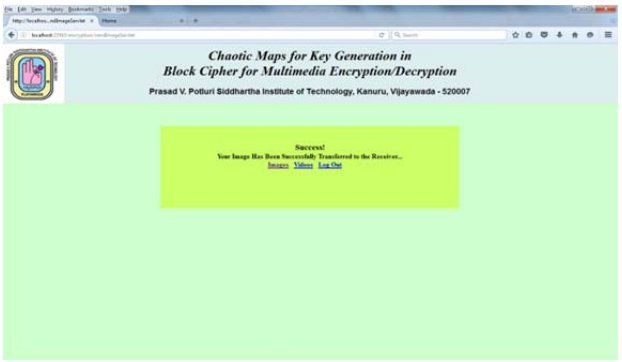

Fig.7. After the image is encrypted, and when requested, image is transmitted from the sender to another user (receiver) via network

Decryption of Image:

After the image is received, the user clicks on the decrypt button, which inputs the cipher image to the decryption system that reconstructs the plain image and is displayed to the user. This is shown in Fig.8.

Fig.8: Whenever a new Image is transmitted, it is received and user is prompted

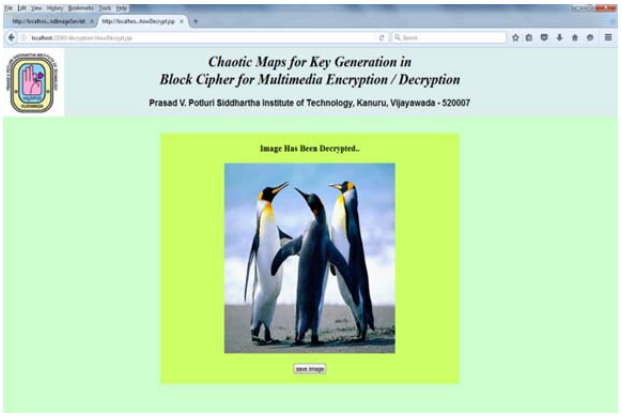

Fig.9: The received image is decrypted and the image is shown to the user

Upload Option:

If the user wishes to process with a new Video, he can click upload new link, and is directed to an option menu, where he/she can select the video to upload from his computer. After the upload completes, the user is directed to the home page again. This is shown in Fig.10.

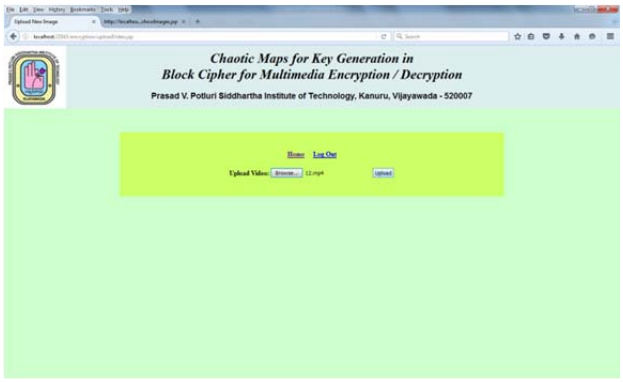

Fig.10. Uploading Video in sender

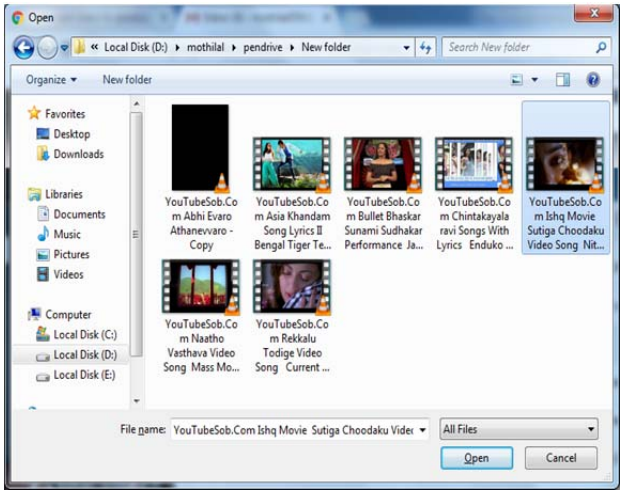

Fig.11. Selecting Video

Encryption and Sending:

After the video is selected, the user can perform encryption on the video by clicking the button below the video details. The video is inputted to the encryption system which produces a cipher video using the proposed key generation algorithm with a simple encryption technique. And the result is displayed as a message to the user and the option to send the encrypted video is shown to the user. When the user hits the button, the encrypted video is sent as packets over the network to the receiver node and the completion of the encryption phase commences with a success message to the user. This is shown in Fig.12.

Fig.12. When User hits the button, the video is encrypted and a relevant message is displayed to the user

Fig.13. After the video is encrypted, and when requested, video is transmitted from the sender to another user (receiver) via network

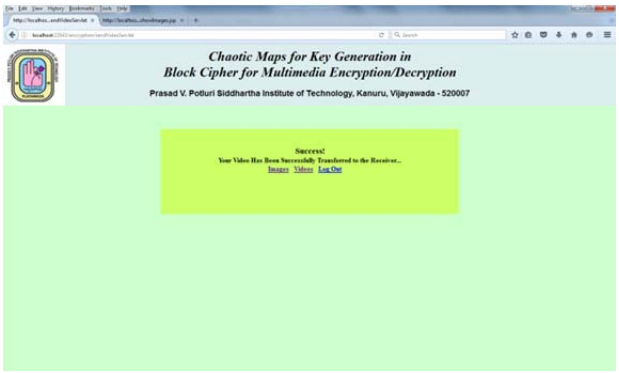

Fig.14. Sending video to the receiver successfully

Decryption of Video:

After the video is received, the user clicks on the decrypt button, which inputs the cipher video to the decryption system that reconstructs the plain video and is displayed to the user. This is shown in Fig.15.

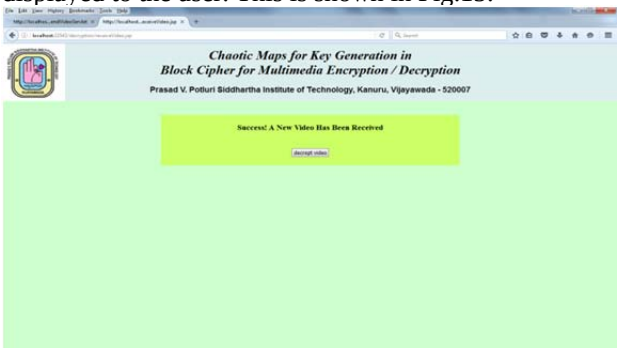

Fig.15. Receiving encrypted video successfully

Fig.16. Decrypting image and saving in receiver database

CONCLUSION

Here we have introduced a new image and video encryption key generation technique based on two keys and implementation with image and video encryption algorithm. This mechanism is useful for providing encryption solution for text as well as multimedia data. The key generation mechanism overcomes the limitations of the previously used symmetric algorithms which have been proven to have several vulnerabilities and can be cracked.

The proposed scheme uses a non-linear chaotic maps approach that provides highly secured and efficient key generation. The security keys K_1 and K_2, have many possible choices which provide the image with a high level of security. The master key can be any binary string with a length of 64 bits. The two session keys produced from the master key are each 64 bit long, and are processed against the input image transformed into bit blocks of 64 bits each.

REFERENCES

[1] Vinod Patidar and K.K. Sud, N.K.Pareek "A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing" Informatica Vol 33, 2009, 441-452.

[2] J. Liu, "Design of chaotic random sequence and its application," Computer Engineering, vol. 3, no. 18, pp. 150-152, 2005.

[3] Yong Xia, Limin Xia, "A New Hyper-Chaotic Algorithm for Image encryption", presented at 9th international Conference for Young Computer Scientists, IEEE, 2008.

[4] Pareek N.K., Patidar Vinod and Sud K.K. "Discereteчatioc cryptography using external secret key" Physics Letters A, vol. 309, pp.2129-2151, 2006.

[5] Yicong zhou,Karen Panetta,Sos Again, "Image Encryption Using Binary key images", Proceedings of the IEEE International Conference on Systems ,Man and Cybernetics,San Anbnio,USA,October,2009.

[6] K. Sakthidasan@Sankaran and B. V. Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011

[7] G.A.Sathishkumar, Dr.K.Bhoopathy bagan and Dr.N.Sriraam, "IMAGE ENCRYPTION BASED ON DIFFUSION AND MULTIPLE CHAOTIC MAPS", IJNSA, Vol.3, No.2, March 2011

[8] A Block Cipher for Multimedia Encryption using Chaotic Maps for Key Generation by P.Vidhya Saraswathi and M.Venkatesulu, 2013.

[9] Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas, Aniket More "Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study", International Journal of Computer Applications (0975 – 8887) Volume 65– No.1, March 2013

[10] Ephin M, Judy Ann Joy, N. A. Vasanthi "Survey of Chaos based Image Encryption and Decryption Techniques", IJCA, Amrita International Conference of Women in Computing (AICWIC'13).

[11] Michael François1, Thomas Grosges1, Dominique Barchiesi1, Robert Erra2, "Image Encryption Algorithm Based on a Chaotic Iterative Process", Applied Mathematics, 2012, 3, 1910-1920.

[12] Deep Desai1, Appoorv Prasad, Jackson Crasto, "Chaos-Based System for Image Encryption", IJCSIT, Vol. 3 (4) , 2012

[13] Saurabh Sharma, Pushpendra Kumar Pateriya, Lakshmi, "A Study Based on the Video Encryption Technique", International Journal of P2P Network Trends and Technology- Volume3Issue1- 2013.

[14] J.A. Gonzailez and R.Pino, "pseudo-random number generator based on unpredictable chaotic functions, Computer Physics Communications, vol.120, no.2-3, pp.109-114, 1999.

[15] L.Wang, F.P.Wang, and Z.J. Wang, "Novel chaos based pseudo random number generator, Acta Physics Sinica.vol.55, no.8, pp.3964-3968, 2008.

[16] A Block Cipher Algorithm for Multimedia Content Protection with Random Substitution using Binary Tree Traversal, P.Vidhya Saraswathi and M.Venkateswarulu, 2012.

[17] Saurabh Sharma, Pushpendra Kumar Pateriya, Lakshmi, A Study Based on the Video Encryption Technique,

[18] http://www.roseindia.com/

[19] http://java.sun.com/

[20] http://www.javadb.com/

[21] http://w3schools.com/

[22] http://stackoverflow.com/

[23] http://www.java2s.com/