IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Implementation and Analysis of Image Base Key Generation and Authentication for Cyber Security

Ms. B. P. Mohod[1], Prof. V. R. Raut[2]

Student, EXTC, PRMIT&R, Badnera, India[1]

Professor, EXTC, PRMIT&R, Badnera, India[2]

Abstract: Information sharing by digital media is a vital and challenging one. These challenges are faced with the help of cryptographic techniques. Cryptography is a progressive technology that Uses key for encryption with plain text. To provide the security of data while communication in cryptography Algorithm and Key are require. The integrity, confidentiality and authenticity of the data in communication depend on algorithm as well as on key. The length of key in cryptography is restricted due to human memorize ability. Only Cryptography is a technique which has a capability to transform the secure information over the internet. The main objective of this paper is to increase the security of communication by providing encryption to the information from the key generated by using an images. Based on the RGB image selected from database a key is generated which is further used for encryption and decryption purpose of the messages which is then transmitted and received between two sides. The AES algorithm is used in this technique on both side for encrypting and decrypting the original message. The generation of key from RGB image(color image)technique is a technique which will work better for key generation than available the traditional key generation method.

Keywords: Cryptography, encryption, decryption and key.

I. INTRODUCTION

The cryptography provides security to the data which is transferred in publically shared media. When cryptography keys are long, it can identify by the attacker, but it will be difficult to remember. The security of cryptographic system relies on the fact that the cryptographic keys are secret and known only to the legitimate user. The communication technologies have major impact in this world hence to ensure security while transferring of information is important. Thus new cryptography approach shows the image based key generate and the encryption and decryption for different data. The proposed system focuses on generating a 16 Byte key based on images. The generated key need not have to be stored. These key can be generated anywhere by using the image and the session of image. This creates more complexity to crack or guess the keys by using the cryptanalysis techniques. To break this algorithm, we need to know the images database, color image channel, the key value and the session type. This method is more secure than traditional cryptographic processes. The algorithm process has an advantages of key generation based on session. This process provides more flexibility that any RGB image can be used for key generation as the key generation is directly based on the image content. To apply more security AES algorithm is used for generating chipper data from the original data and to get original data back again apply AES decryption algorithm on encrypted data. Color image values are taken and processed for 16 byte key generation. There by it is able to creates a complex system for cracking and easy way to implement. This algorithm focused on the image data based security. According to literature survey and research done it can be found that AES algorithm is most efficient in terms of speed, time and throughput.

II. LITERATURE SURVEY

“A Novel Cryptography Method Based on Image for Key Generation”. Tawfiq S.Barhoom et al.
In this paper they have proposed and produced an experimental result on the method which is more secure than traditional cryptographic processes. Cryptography provides security to the data which is transmitted between the communicators through a shared media. When the keys used for the encryption and decryption are too long, it is difficult to be remembered and unable to guess by the attacker. Storing the secret key in a database or in a file is insecure. The security of the cryptographic system relies on the fact called cryptographic keys which are secret and known only to the authorized user. Thus the new concept of Cryptography is being determined based on the key generated directly from an image stored in the database and the process of key generation is based on sessions. This method creates more complexity to crack or guess the keys by using the cryptanalysis techniques .So it impossible to break the algorithm unless we know the

DOI 10.17148/IJARCCE.2016.511107

image from database, color image channel, the key value and the session type. This process has an advantage that key length varies according to the length of the message and it is more flexible on any RGB images.[1]

“A Novel Cryptographic Key Generation Method Using Image Features” B.Santhi et al.
They have proposed a method which overcome the disadvantages of several methods such as steganography and cryptography which deals with difficult in the size of information to be transferred and with encryption using the keys which is difficult in remembering and can be easily cracked. Thus, the author has determined the concept which should be flexible and should not be compromises in the strength of key generated and information security, their by proposing the secret key which is being generated from an image. Using the Gray Level Co-occurrence properties of the image, a 56-bit sub-key is generated. Therefore the sub- key is initialized as secret key to the encryption and decryption of the message which is to be transmitted securely and efficiently between the communicators. The strength of the key is much better than the key generation process of other algorithms because the key is based on the image properties, which is impossible to predict.[2]

“Efficient Cryptographic Key Generation Using Biometrics”. Dr.R.Seshadri et al.
They have proposed an efficient cryptographic key generation algorithm using biometrics. As the conventional cryptographic keys are large they are very difficult to remember. Hence they have integrated biometrics like fingerprint, face, voice, iris etc. along with cryptography for an efficient secure key generation. In this paper finger prints are used for generating cryptographic keys. Finger print patterns are used for key generation as they are stable for a person’s life time. Three models are used in the proposed system they are key release, key binding and key generation. In key release mode the key and the biometric are stored separately in a template and the key will be released only if the biometric matches. In key binding mode a cryptographic biometric matching algorithm is used for authentication and key release. In key generation mode key is generated based on the biometric data directly and it s not stored in the database.[3]

“A Novel Key Generation Cryptosystem Based on Face Features” Lifang Wu et al.
They have proposed an algorithm to share the pictures through a shared medium. Face biometrics is the most effective biometric feature universally known because it uniquely identifies the differences in the face features. During the encryption phase the face key features are extracted. Based upon the optimal bit order and the binarization which are saved in the look-up table the bio-keys are generated. The generated bio keys are then encrypted. The face images are unequalled because of the noise in the camera. It is solved by error-correct- code (ECC). While transmitting from the sender side the encrypted message is sent with the ECC code. At the receiver end the decrypted data is obtained using ECC code and the bio-keys are generated back with the help of the look-up table. By this approach a secure and stable binary key is generated for the transmission of images.[5]

“CryptoStego-A Novel Approach Creating Crypto - graphic Keys and Messages” Damir Omerasevic et al
They have proposed an algorithm in which the plaintext is shared with the help of images by establishing the cryptographic key. The size of the key and the space is limitless. The main objective of the paper is to share messages with the help of multimedia files. Any multimedia file of bigger size compared to the messages is chosen. The sender will choose an image from the set of images and selects the position for attaching the plain text. The plain text is then XOR-ed with the set of selected bits in the image and sent to the receiver with the details of the position of file and the index. Each message is encrypted separately with the unique key which is similar to one time padding. Selecting the multimedia file and the position where the plaintext is to be attached is selected using an algorithm. This method generates cryptographic keys that are not based on any particular size.[6]

III. DRAWBACKS OF PREVIOUS SYSTEM

The size of color image is always greater than that the size of text. Therefore, cryptography required much time to encrypt data of image. Where in secure communication, the phase of key generation has many challenges and this problem can be solved if the key is share in any form between the sender and the receiver or if the generation of the keys takes place rapidly during encryption and decryption separately, thus, the concept of generation of the key from an color image came to the role.

IV. APPROACH FOR IMAGE BASE KEY GENERATION

There are 4 main steps while performing a image base key generation and encryption process. The step’s are database creation, key generation, data encryption data decryption.

i) Data base creation:- In this phase as we are going to use sessions based key generation so twenty four images are used on hourly basis session. The images are the set of a color image i.e. RGB image. Once the sender and the receiver are ready for communication they have access to the image data base the sender and receiver should use same image databases and an image with both users should be of same name. Only legitimate sender and receiver can access the image database.

ii) Key generation: - Key is generated from the color image stored in database based on the different type of image, the selection of image is randomly done. The randomly done selection of image is inform to user by encrypting it’s name and transmitting it with encrypted message in file. In this paper we used one plane of RGB

DOI 10.17148/IJARCCE.2016.511107

color image red, green or blue. So we have to shuffle image 4*4 block matrix vertically up shift and horizontally left shift increase step by step by matrix form and select R plane 8 byte or G plane 4 byte and B plane 4 byte to get 16 byte key. The method uses a RGB image to generate a key which will be used in the encryption and decryption operations.

iii) Encryption: - The sender encrypts the confidential message using the AES algorithm. In this level AES-128 bit encryption algorithm is used. The AES standard states that the algorithm can only accept a block size of 128 bits. In this case the entire data block is processed is parallel during each round using substitutions and permutations. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10. The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption. The exception that each stage of a round its counterpart in the encryption algorithm. The four stages are as follows: 1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

iv) Decryption:- According to the session log the receiver will consider the image in the image database and generate key from that image which is used for decryption. The generated key and the encrypted message both are send for decryption (AES Algorithm) and the original message is extracted. In this level the AES-128 bit algorithm is used. The algorithm steps are as follows. The tenth round simply leaves out the Mix columns stage. The first nine round of the decryption algorithm consist of the following.

- Inverse Shift rows
- Inverse Substitute bytes
- Inverse Add Round key
- Inverse Mix columns.

V. RESULT

The result for several inputs with an output is shown in table below.

Sr. No.	INPUT TEXT	IMAGE NAME FOR KEY GENERATION	GENERATED KEY	ENCRYPTED TEXT(Cipher Text)	DECRYPTED TEXT(Plain Text)
1.	Gmail provide communication facility.	Desert	2F 34 35 3A 40 47 43 3C 7C 7C 7E 7D CE CE CD CC	J"æ÷Sŧ-Ð-ŔÈõ-e(z/,èE-ÿ?- ķü--h\	Gmail provide communication facility.
2.	Encryption convert plain text into cipher text	girl	09 09 09 08 09 09 09 09 11 11 11 10 QA QA QA 09	-0ð4Ë¸ıĐ¤\ÕaH¤]_|-|-ãa2Ø«Ð-Ɵ	Encryption convert plain text into cipher text
3.	Decryption convert cipher text into plain text	Hydrangeas	01 01 01 00 01 00 00 00 14 14 14 13 00 00 01 00	üıé'ËX ?ıüaÇã«Â-Ã0-Ë¹Ã¼µ¯a-Ã°Hnd@ü	Decryption convert cipher text into plain text
4.	Key is important factor in cryptography.	Lighthouse	70 6F 6F 6B 6A 6C 6C 6F 91 90 90 8E C6 C5 C6 C4	Θ±±7ř- -FQü-\$2Ǯy@ˆAi¿¡ÜE¹ieðB¾mN	Key is important factor in cryptography.
5.	Image has three plane.	Koala	65 67 6E 68 68 68 6C 64 5A 5C 5F 5B 3A 3E 42 3B	Q-¸ÕðWG-EÄR˜-upi Ö	Image has three plane.

VI. ANALYSIS OF PROPOSED SYSTEM

The performance analysis can be done with various measures such as Diffusion analysis of AES & avalanche effect, Speed comparison with encryption and decryption cycles, key setup and key initialization and throughput of encryption and decryption. The performance analysis will be presented in the form of tables and figures as below.

A. Diffusion analysis

Diffusion is made for AES in two condition as listed below:-
1. Changing a key at a time, keeping plain text as constant.
2. Changing a plain text at a time, keeping key as constant.

The output for an above two case is shown in table 1 and table 2. From table 1 and table 2 we can see that Diffusion is made for AES in two conditions as exhibits a strong change in the output. This strong change shows that for simple change in key or input text as result large change so it offers a more security. Overall it is identified that AES can be used in circumstances where high security is required. Also AES is very much suitable for widespread smart card implementation there is need for high security.

B. Time analysis

The time analysis contain the three type time analysis i.e. Initialization time analysis, Encryption time analysis, Decryption time analysis. This time analysis further used for to calculate a average time and throughput of system. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. Different packet sizes are used in this experiment for both AES algorithms. The encryption time is recorded for the encryption algorithms. The average data rate is calculated for AES algorithm based on the recorded data. The formula used for calculating average time is shown below.

$$AvgTime = \frac{1}{Nb}\sum_{I=1}^{Nb} \frac{Mi}{ti}(Kb/s)$$

Where
Avg Time = Average Data Rate (Kb/s)
Nb = Number of Messages
Mi=Message Size (Kb)
Ti=Time taken to Encrypt Message Mi

Encryption time is also used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated using the following formula

$$\text{Throughput} = \frac{T_P}{E_t}$$

Where Tp= Total Plain text
Et= Encryption time

The result for Encryption time, Decryption time and Initialization time is shown in Table 1 and table 2 . It is very important to calculate the throughput time for the encryption algorithm to known better performance of the

DOI 10.17148/IJARCCE.2016.511107

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 11, November 2016

algorithm. The average time required for the system by calculating the result is 142.2 millisecond where the throughput of the system is 18.

Sr. No.	Input text	Input image	Cipher text	Time for execution (milisecond)		
				Initiali-zation time	Encryption time	Decryption time
1.	Sky is Blue.		ûñNÖvë¤ ã0	1.576081	0.019118	0.019118
2.	Sky is Blue		<e[┴¬y\ë²ò0	1.555529	0.019088	0.019088
3.	Sky is Blue		┼•æ±ÿÆxå	1.570981	0.019427	0.019427
4.	Sky is Blue		¿=-'W©$·ùV	1.575610	0.019385	0.019385
5.	Sky is Blue		é─┤ÉãäGNLë	1.654683	0.024234	0.024234

Table 1: Change in key.

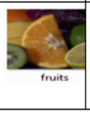
Sr. No .	Input text	Input image	Cipher text	Execution time		
				Initial-ization time	Encryption time	Decryption time
1.	Information secured in image		[illegible]	1.608589	0.036513	0.036513
2.	There is no success like failure		Údr®-cuª-v-Áûü_3 ïΓÝî½Ø¯ø7×LÀ-	1.593245	0.036829	0.036829
3.	Old media is dead media		)w®¥-=É¡|•¹ť:ˆã-¿─zDd	1.560346	0.036001	0.036001
4.	all things are possible given enough time		[illegible]	1.582725	0.053227	0.053227
5.	We are the change.		uù─┤½zÖ/åo@ G#²	1.606244	0.036051	0.036051

Table 2: Change in input text

VII. CONCLUSION

The communication technologies have major impact in this world, security while transferring of information is important. Our proposed system focuses on generating key based on images. The generated key need not have to be stored. It can be generated anywhere using the image and the session. This creates more complexity to crack or guess the keys by using the cryptanalysis techniques. To break this algorithm, we need to know the images database, color image channel, the key value and the session type. This method is more secure than traditional cryptographic processes.AES algorithm is ued for encryption and decryption.

REFERENCES

[1] Tawfiq S.Barhoom, Zakaria M.Abusilimiyeh, "A Novel Cryptography Method Based on Image for Key Generation". Proceedings on the Palestinian International Conference on Information and Communication Technology, 2013-IEEE, pp: 71-76.

[2] B.Santhi,K.S.Ravichandran,A.P.Arun and L.Chakkarapani, "A Novel Cryptographic Key Generation Method Using Image Features". Proceedings on the Research Journal of Information Technology2nd International Conference on Adaptive Science & Technology, 2012, Pp: 88-92.

[3] Dr.R.Seshadri, T.Raghu Trivedi, "Efficient Cryptographic Key Generation Using Biometrics". Proceedings on the International Journal on Computer Technology and Application, ISSN: 2229-6093, Vol-2, Pp:183-187

[4] Amrita Sahu, Yogesh Bahendwar, Swati Verma, Prateek Verma, "Proposed Method of Cryptographic Key Generation for securing Digital Image". Proceedings on the International Journal of Advanced Research in Computer Science and Software Engineering, 2012, Pp: 285-291.

[5] Lifang Wu, Xingsheng Liu,Songlong Yuan, Peng Xiao Tawfiq S.Barhoom,Zakaria M.Abusilimiyeh , "A Novel Key Generation Cryptosystem Based on Face Features". Proceedings on ICSP, 2010-IEEE, Pp:1675-1678.

[6] Damir Omerasevic, Narcis Behlilovic, Sasa Mrdovic,"CryptoStego-A Novel Approach for Creating Cryptographic Keys and Messages", 2013-IEEE, Pp: 83-86.

[7] Saksham Wason,Piyush Kumar,Shubham Rathi,"Text and image encryption using color image as a key" Internatonal Journal Of Innovative Research In Technology 2014 IJIRT | Volume 1 Issue 5 | ISSN: 2349-6002.

[8] Mohammed Tajuddin, C. Nandini ,"Cryptographic Key Generation using Retina Biometric Parameter" International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013.

[9] M. S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "Crypto key generation using contour graph algorithm", in the 24th IASTED international conference on Signal processing, pattern recognition, and applications (SPPRA'06), M. H. Hamza (Ed.). ACTA Press, Anaheim, CA, USA, pp. 95-98, 2006.

[11] Asha Ali, LiyamolAliyar andNisha V K, "RC5 Encryption Using Key Derived From Fingerprint Image", Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference, 28-29Dec. 2011.

[12] Priyanka.M, Lalitha Kumari.R, Lizyflorance.C and John Singh. K "A New Randomized Cryptographic Key generation Using Image"International Journal Of Engineering Science and Innovation Technology(IJESI) Volume 2,Issue6,November2013.

[13] William Stallings, Cryptography and Network Security, Person Education 3rdEd, Wiley, 1995

[14] Advance encryption standard (AES) Federal Information Processing Standards Publication (FIPS PUBS) are issued by the National Institue of standards and Technology, November 26,2001

[15] Murli ,P. I and R.Palraj , "true random number generation method based on image for key exchange algorithm",2009 International Symposium on Computing Communication ,and Control

[16] Ahmad Amro, El-Sayed M. El-Alfy,"Known-Plaintext Attack and Improvement of PRNG-Based Text Encryption" 2016 7th International Conference on Information and Communication Systems (ICICS),978-1-4673-8614-2/16/@2016 IEEE.

[17] Akash Kumar Mandal, Chandra Parakash, Performance Evaluation of Cryptographic Algorithms: DES and AES, Conference on Electrical, Electronics and Computer Science,,978-1-4673-1515-9/12/@2012IEEE

DOI 10.17148/IJARCCE.2016.511107