IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Securing Secret Messages: A Review

Anil C.[1], Anuradha S.[2], Arpita V. Murthy[3], Sridevi S.[4], Guruprasad M. Bhat[5]

Department of Electronics and Communication, Jyothy Institute of Technology, Bengaluru[1,2,3,4,5]

Abstract: Due to advancements in technology, most of the operations are now being conducted on server/cloud. But this increases the potential threat of data leakage by hackers. Thus, in order to secure the data, many steganographic and cryptographic methods have been proposed. An overview of these systems has been reviewed in this paper.

Keywords: Steganography, Cryptography, Visual Cryptography, AES, DES, Triple DES, TDES, 3DES.

I. INTRODUCTION

Technology has changed our lives in many aspects – from the advent of natural user interfaces [1], [2], safeguarding our lives [3], and in helping those who are physically weak/challenged [4], [5], [6] and also to be it in the case of helping physically challenged. It has also changed the mode of communication from hand-written letters to wired communication to wireless [7], [8], [9]. Now-a-days, most of the communication modes are dependent on Internet. Even the secret messages are being stored and sent through servers.

I t has been witnessed in the recent history, that many of the sensitive secret information related to Governments, Defence and Banks have been hacked and leaked on the Internet [10]. This unauthorized leakage of data from a classified source is called Data Leakage or Information Leakage [11]. Thus in order to secure the data, many researchers such as [12], [13] have put in their efforts to secure the data. Most of the data gets leaked during the transmission of the data from a source to a destination. Thus, methods such as steganography and cryptography are employed to secure the data [14]. This paper discusses about different methods that are used to secure the sensitive data.

This paper has been into five sections. Section 2 discusses about Steganographic methods and Section 3 deals with details of Cryptography. Section 4 compares all the methods. Section 5 concludes the paper.

II. STEGANOGRAPHY

Steganography is the process of hiding a data into another data [15]. The most popular type of steganography is image base, where data is hidden in the images. Watermarking and Visual Cryptography are the two well known methods that are employed from Image Steganography.

A. Watermarking

The message image is embedded inside a protective image called "Cover Image" and is transmitted to the recipient. In order to get back the message content, the reverse process of Watermarking has to be done. The simplest form of Watermarking is the Least Significant Bit on an 8-bit image [16]. Here, the 4 LSBs of the cover image are replaced by the 4 MSBs of the image that has to be hidden.

B. Visual Cryptography

Visual Cryptography is the process of encoding the secret image into two shares and transmitting them [17]. At the receiver, the two shares have to be combined to get back the message. These shares appear random and contain no decipherable information about the underlying secret image, however if any 2 of the shares are stacked on top of one another the secret image becomes decipherable by the human eye, i.e. retrieving the secret image becomes a mechanical process.

III. CRYPTOGRAPHY

Cryptography is all about securing the content. In cryptography, encryption is the process of encoding messages or information in such a way that only authorized recipient can read it [18]. Encryption not only prevents interception, but also denies the message content to the interceptor. In this technique, the intended message is encrypted by using an encryption algorithm, which uses pseudo-random encryption key to generate a cipher text. This generated key is known only to the message originator and the recipient.

Decryption is the technique of decoding the encrypted information such that is can be accessed again by authorized recipients only [19]. This is considered as the reverse process of encryption. An authorized recipient can decrypt data only if he has the confidential key employed while encrypting the data.

The encryption strength is usually measured by the key size. The encrypted data can be subjected to brutal force attacks in which all possible combinations are tried, no matter how strong the encryption algorithm may be. The time taken to crack the most modern ciphers of decent key lengths with brutal force is measured in millennia. Usually the length of the key should be suitable for securing the data for a reasonable amount of time.

The most commonly applied encryption standards are Data Encryption Standard (DES), Triple DES, and Advanced

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Encryption Standard (AES) [20], [21], [22], [23], [24], [25].

A. Data Encryption Standard (DES)

DES is the standard that was originated by the U.S. government, which began promoting for both business use and government. A 56-bit key is generated for encrypting high sensitive information. However, it is acceptable for lower security applications and hence used in many commercial products. It is also used in products that have slower processors, such as appliance devices that can't process a larger key size and smart cards.

DES takes a fixed length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. Block size in case of DES is 64 bits. Initially, the block is divided into two 32-bit halves and processed alternatively; this criss-crossing is known as the Feistel scheme. The F-function combines half a block together with some of the key. Overall Feistel structure consists of 16 identical stages of processing called rounds. The initial and final permutation, termed IP and FP respectively works in inverse to each other but has no cryptographic significance. The output of the F-function is jumbled with the other half of the block, and the halves are swapped before sending to the next round. After the final round, the block halves are swapped. This is the main feature of Feistel structure which makes both encryption and decryption similar processes. The ⊕ symbol denotes the XOR operation.

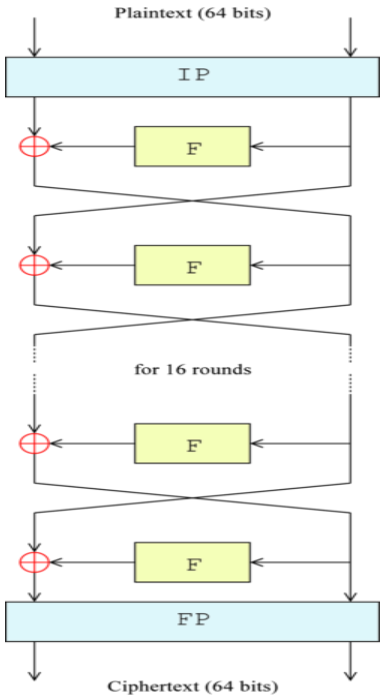

Fig 1: Overall Feistel structure of DES

B. Triple DES

The higher and improved version of DES is known as Triple DES, or 3DES as it is sometimes written, and its name implies what it does. At the transmitter, the data is first encrypted, then decrypted and again encrypted with the three different keys. At the receiver, in order to decrypt the data, the received data is decrypted, then encrypted and again decrypted with the same keys. This method does not give an increase in the strength of the cipher because the first encryption key is used twice to encrypt the data and then a second key is used to encrypt the results of that process, but an effective key length of 168 bits is plenty strong for almost all uses.

C. Advanced Encryption Standard

The U.S. government began to search for a replacement for the DES due to eventual end of its useful life. The Government standard body and National Institute of Standards and Technology (NIST) announced an open competition for a new algorithm that would become the new government standard. Two Belgian cryptographers introduced AES, which was based on an algorithm called Rijndael. AES is becoming rapidly the new standard for encryption. It offers up to a 256-bit cipher key, which is more than enough power for the future. Typically, for performance considerations, AES is implemented in either 128- or 192-bit mode.

AES belongs to a family of ciphers which has fixed block size of 128 bits and a key size of 128, 192 or 256 bits. AES operates on a 4×4 matrix of bytes, termed as STATE. For an instance, if there are 16 bytes, b0, b1,……., b15, these bytes are represented in the form of matrix as:

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

Fig 2: An example for block size

In AES, key size represents the number of repetitions of transformation rounds that convert the plaintext, into the cipher text. The number of cycles of repetition for 128-bit, 192-bit and 256-bit keys is 10, 12 and 14 cycles respectively.

The following are the steps involved in AES: Adding round key, Sub Bytes, Shifting Rows and Mixed Column. Initially, the round keys are obtained from the cipher key according to the Rijndael's key schedule. AES requires a separate 128-bit round key block for each round.

In "Adding Round Key" step, each byte of the state matrix is combined with a byte of the round sub key using the XOR operation, as depicted by Fig 3. Sub Bytes is a non-linear substitution step where each byte is replaced with another using a look up table. In this step, each byte in the state matrix is replaced with its entry in a fixed 8-bit lookup table, as shown in Fig 4. In Shift rows method, the last three rows of the state matrix is shifted cyclically a certain number of times, as shown in Fig 5. The bytes in each row are shifted cyclically to the left. The number of

DOI 10.17148/IJARCCE.2016.5578

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

places for shifting each byte differs for each row. Next, in Mixed Column approach, each column of the state matrix is multiplied with a fixed polynomial c(x), as shown in Fig 6.

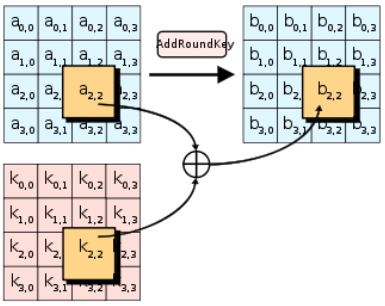

Fig. 3: Adding round key

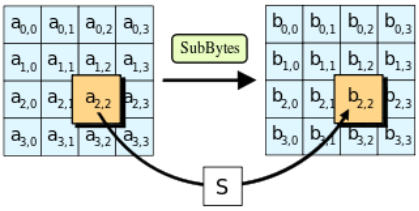

Fig 4: Replacing values using look up table – Sub Bytes

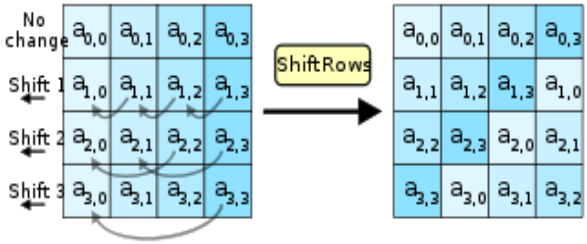

Fig 5: Shifting Rows

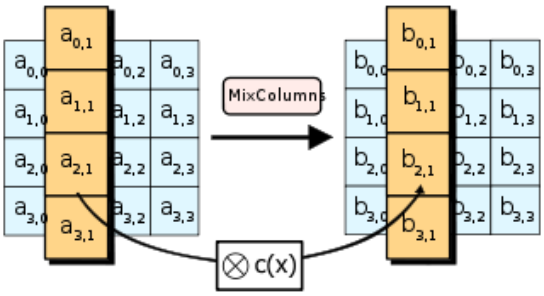

Fig 6: Mixed Column

AES does encryption on the state matrix in different rounds like key expansion, initial round (adding round key), main round (sub bytes, shifting rows & mixing columns), and final round (main round except mixing of columns).

IV. COMPARISON

The Advance Encryption Standard (AES) and Triple DES (TDES or 3DES) are the most commonly used block ciphers. Either of the technique can be used that depends on our needs. Their differences are highlighted in terms of security and performance in this section. DES and 3DES techniques involve more of bit manipulation in 16 rounds in each substitution and permutation boxes. The data in DES is encrypted in 64 bit block size and a 56 bit key is used effectively. 56 bit key corresponds to 72 quadrillion possibilities approximately. It seems large but according to today's computing power it is not sufficient and vulnerable to brute force attack. Therefore, DES is no longer appropriate for security and could not keep up with advancement in technology. Thus, 3DES was introduced, which works on 3 keys, giving the effective key length of 168 bits.

The comparison between AES and DES is illustrated in Table 1. Due to the advantages of AES over DES, AES is used for encrypting passwords and other sensitive information.

TABLE I: COMPARISON BETWEEN AES AND DES

Factors	DES	AES
Key size	56 bits	128,192 or 256 bits
Block length	64 bits	128,192 or 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Cryptography analysis Resistance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and square attacks
Keys possible	256	2128, 2192 and 2256
ASCII Printable Character Key possible	957	9516, 9524 or 9532

V. CONCLUSION

Even though the above mentioned methods have been implemented for data security, hackers have managed to break through these barriers and get the data. Thus, in order to make the information more secure the steganography and the cryptography methods can be used together.

ACKNOWLEDGMENTS

Our sincere thanks to **Mr. Sudhir Rao Rupanagudi** from WorldServe Education, for contributing towards development of this work.

REFERENCES

[1]. P. C. Ravoor, B. S. Ranjani and S. Rao Rupanagudi, "Optimized fingertip blob recognition for image processing based touch-screens," Recent Advances in Computing and Software Systems (RACSS), 2012 International Conference on, Chennai, 2012, pp. 104-108.

[2]. P. C. Ravoor, S. R. Rupanagudi and B. S. Ranjani, "Detection of multiple points of contact on an imaging touch-screen," Communication, Information & Computing Technology (ICCICT), 2012 International Conference on, Mumbai, 2012, pp16.

[3]. S. R. Rupanagudi et al., "A novel video processing based smart helmet for rear vehicle intimation & collision avoidance," 2015 International Conference on Computing and Network Communications (CoCoNet), Trivandrum, 2015, pp. 799-805.
[4]. Rupanagudi SR, Bhat VG et al (2015) Design and Implementation of a Novel Eye Gaze Recognition System Based on Scleral Area for MND Patients Using Video Processing. Advances in Intelligent Informatics. doi:10.1007/978-3-319-11218-3_51
[5]. Rupanagudi SR, Bhat VG et al (2015) Design and Implementation of a Novel Eye Gaze Recognition System Based on Scleral Area for MND Patients Using Video Processing. Advances in Intelligent Informatics. doi:10.1007/978-3-319-11218-3_51
[6]. S. R. Rupanagudi et al., "A novel video processing based cost effective smart trolley system for supermarkets using FPGA," Communication, Information &Computing Technology (ICCICT), 2015 International Conference on, Mumbai, 2015, pp.1-6.
[7]. S. R. Rupanagudi et al., "Design of a low power Digital Down Converter for 802.16m - 4G WiMAX on FPGA," Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on, New Delhi, 2014, pp. 2303-2308.
[8]. S. R. Rupanagudi et al., "A low area & low power SOC design for the baseband demodulator of an indoor local positioning system," 2015 International Conference on Computing and Network Communications (CoCoNet), Trivandrum, 2015, pp. 689-695.
[9]. S. R. Rupanagudi, Ranjani B. S., P. Nagaraj, V. G. Bhat and Thippeswamy G, "A novel cloud computing based smart farming system for early detection of borer insects in tomatoes," Communication, Information & Computing Technology (ICCICT), 2015 International Conference on, Mumbai, 2015, pp. 1-6.
[10]. US Government faces pressure after biggest leak in banking history, The Guardian (Accessed on April 10, 2016) [Online]. Available: http://www.theguardian.com/news/2015/feb/08/us-government-biggest-leak-banking-history-questions-irs-taxes
[11]. Sans Institute (2007), Data Leakage – Threats and Mitigation [Online]. Available: https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931
[12]. S. R. Huddar, S. R. Rupanagudi, R. Ravi, S. Yadav and S. Jain, "Novel architecture for inverse mix columns for AES using ancient Vedic Mathematics on FPGA," Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on, Mysore, 2013, pp. 1924-1929.
[13]. G. l. Guo, Q. Qian and R. Zhang, "Different Implementations of AES Cryptographic Algorithm," High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on, New York, NY, 2015, pp. 1848-1853.
[14]. Sarmah D.K., Bajpai, N., Proposed System for data hiding using Cryptography and Steganography. [Online] Available: https://arxiv.org/ftp/arxiv/papers/1009/1009.2826.pdf
[15]. Kumar, A., Pooja, Km., "Steganography- A Data Hiding Technique" in International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.
[16]. What is Steganography [Online] Available: https://www.clear.rice.edu/elec301 /Projects01/ stegosaurus /background. html
[17]. J. Ramya and B. Parvathavarthini, "An extensive review on visual cryptography schemes," Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on, Kanyakumari, 2014, pp. 223-228.
[18]. Xun Yi, Russell Paulet, Elisa Bertino (2014) Homomorphic Encryption and Applications, Springer Publications, Ch 1, pp 1
[19]. H. Lee Kwang, Basic Encryption and Decryption [Online]. Available: http://www.apprendre-en-ligne.net/crypto/bibliotheque /PDF/Kwang.pdf
[20]. Man Young Rhee, Internet Security: Cryptographic Principles, Algorithms and Protocols, John Wiley & Sons, 2003, Ch 3, pp 82
[21]. Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition. ISBN: 978-0-470-06852-6. Ch 5, pp 73-114.
[22]. A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "NovelApproach for Cover File of Hidden Data in the Unused Area Two within EXE File Using Distortion Techniques and Advance Encryption Standard.", Proceeding of World Academy of Science Engineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P 498-502.
[23]. M. Abomhara, Omar Zakaria, Othman O. Khalifa , A.A.Zaidan, B.B.Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard ", International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198,Vol.2 , NO.2, April 2010, Singapore..
[24]. A.W. Naji, Shihab A. Hameed, B.B.Zaidan, Wajdi F. Al-Khateeb, Othman O. Khalifa, A.A.Zaidan and Teddy S. Gunawan, " Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standared and Distortion Techniques", International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, P.P 73-78,3 Aug 2009, USA.
[25]. Hamdan. Alanazi, Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, "New Frame Work of Hidden Data with in Non Multimedia File", International Journal of Computer and Nsetwork Security, 2010, Vol.2, No.1, ISSN: 1985-1553, P.P 46-54,30 January, Vienna, Austria.