Vidhyayana - ISSN 2454-8596

An International Multidisciplinary Peer-Reviewed E-Journal

www.j.vidhyayanaejournal.org

Indexed in: ROAD & Google Scholar

Design and implementation of a new encryption algorithm in MATLAB for multimedia files

Riddhi Somaiya

Ph.D. Scholar, Department of Computer science
Saurashtra University, Rajkot, India

Dr. Atul Gonsai

Professor, Department of Computer Science
Saurashtra University, Rajkot, India

Rashmin Tanna

Lecturer, Electronics and Communication department,
AVPTI, GTU
Rajkot, India

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

ABSTRACT

Transmission of digital content has increases tremendously these days. Privacy and security of the transmitted data has become an important concern in multimedia applications because multimedia data has been an essential part of our lives, from instant messaging applications to social media. For security of the data we use different techniques like cryptography, steganography, and scrambling. Cryptography is one of the main techniques used for information security which includes many forms like digital signatures, authentication etc. and performs system security, confidentiality, data integrity and other functions. This paper works on dual layer security systems using (Elliptic-Curve cryptography) ECC and (Modified Advanced Encryption Standard) MAES called EMAES on Multimedia files (Text, Audio, and Video). Using this approach, unauthorized viewing of the multimedia file can be prevented. Also, this algorithm provides a high level of security and efficiency as compared to existing ones. Comparison of results with other algorithms using parameters like SSIM, FSIM, PSNR and execution time shows that all these parameters are improved 20% or more. The implementation is carried out in MATLAB 2018a.

Keywords: Cryptography, RSA, ECC, AES, MAES, IDEA, hybrid algorithm, EMAES.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

INTRODUCTION

Internet's growing popularity has grown the advent of multimedia transfer applications. Many of those applications require the high security of videos or images transferred, such as video-on-demand, pay-tv to name a few. The Internet, in its present form, does not provide multimedia communication protection up to the mark. Multimedia encryption is therefore essential for absolute confidentiality. Classic algorithms such as RSA, AES, MAES, ECC and IDEA etc., are computationally ineffective for video content. They take a long time to encrypt huge video files. Many encryption algorithms use a simple scrambling mechanism to decrease the encryption time [2].

There are a number of types of data which can be defined as types of multimedia data. Usually these are the components for the building blocks of generalized multimedia environments, networks, methods for integration. The basic types can be represented as objects like text, images, audio, video and Graphic. Multimedia finds its use in numerous fields including, but not limited to, advertising, fashion, education, entertainment, engineering, medicine, mathematics, industry, scientific research and temporal space applications [14].

Cryptography and Steganography are two main methods of ensuring safe communication. Cryptography transforms the message into some gibberish form and Steganography hides the message into several other media files which can be text, image, audio, video etc. Cryptography scrambles the message, so that it becomes difficult to decipher the message and steganography hides the message's presence so that the message isn't obvious[13].

This paper designs and implements a hybrid of modified AES and ECC encryption algorithms called EMAES in MATLAB 2018a used for cryptography. The hybrid algorithm is designed to encrypt any multimedia file such as audio, video, images and text by converting them into a text equivalent to reduce the overall time constraint. Also the security and efficiency both are increased by combining key encryption using ECC and modified AES for data

encryption. It is compared with different algorithms like RSA, ECC, AES, RSA+ECC, etc... On the basis of parameters like SSIM, FSIM, PSNR, execution time etc... It is observed that EMAES has shown improvement of about 20% in almost all the parameters. Different types of attacks and reverse engineering is also tested and found good results.

CRYPTOGRAPHY

Cryptography is an art of translating a message into an encoded unreadable form, so that it can be read and processed only by the intended receiver. The cryptography's main aim is to provide data protection from unauthorized access. The cryptography is composed of encryption and decryption. The translation of the original message into the format is called encryption, which is almost impossible to interpret without the correct understanding. Decryption is the reverse encryption technique. It is the conversion of an encrypted message back to readable original format. Both encryption and decryption involve the use of some confidential information i.e. key [10].

Many of the words used in cryptography:

Plaintext: - This is the original text message.

Encryption: - This is the process of encoding the content of the original message so that the attacker or any outsider does not understand the actual message.

Decryption: - The recovery process copies the original message. Hash Functions: - Generate message digest. Cipher Text: - cipher text is considered encoded text [13].

There are three methods of Cryptography:

- Symmetric-key cryptography.
- Asymmetric-key cryptography.
- Hash functions

Symmetric-key cryptography: for both encryption and decryption, same secret key is used [10].

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

Symmetric key encipherment (also called secret key cryptography) in this same key is used both for encryption and decryption [13].

Asymmetric-key cryptography: There are two separate keys, i.e. one for encryption and one for decryption [10].

Asymmetric key encipherment (also called public key cryptography) is used for encryption in these two separate keys and other for decryption [13].

Digital signature hash function is often used. For message authentication the hash function has become the preferred method in many applications[13].

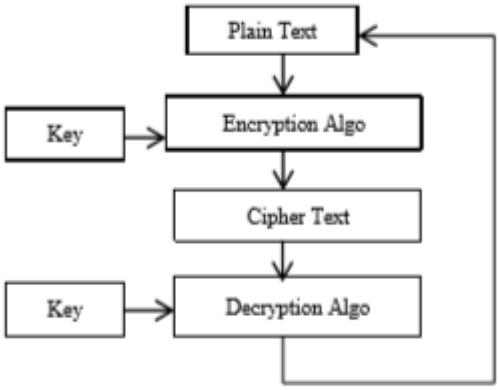


Figure 1: Basic Cryptograph Encryption and Decryption [13]

TECHNIQUES USED TO ENHANCE THE SECURITY OF MULTIMEDIA DATA

A. Rivest-Shamir-Adlemann (RSA)

RSA algorithm, named after the inventors, is the first algorithm that can be used both for data encryption and for the protection of digital signatures. RSA algorithms relies on the complexity of large numbers decomposition. Two large prime numbers are used in algorithms to build the public-key and the private-key. The difficulty of guessing the plaintext from the signal key and the cipher text is estimated to be equal to the decomposition of two large prime numbers [7].

B. Elliptic-Curve Cryptography (ECC)

Elliptic curve based algorithms use slightly smaller key sizes than the variants of the non-elliptic curve. The disparity in the corresponding key sizes increases significantly with

rising key sizes. ECC is a public key cryptography (PKC) that has authentication keys, both public and private. Over finite fields it is based on elliptic curves [8].

C. Advanced Encryption Standard (AES)

AES is a symmetric encryption standard. AES allows One hundred and twenty eight bits of Data Length. AES goes through ten rounds for One hundred twenty-eight-bit keys, twelve rounds for one hundred ninety-two-bit keys and fourteen rounds for two hundred fifty-six-bit keys. AES data length of one hundred and twenty eight bit is divided into four operational blocks and handled as array of bytes, arranged as matrix of 4*4 called State. AES is the most effective algorithm to ensure security in transmission of message [10].

D. Modified Advanced Encryption Standard) (MAES)

Optimization of Advanced Encryption Standard can be done and efficiency could be increased by removal of sbox generation and polynomial matrix generation processes and modification in mix column process. The unnecessary complex multiplication process can be replaced by simple mapping process. Results show that percentage improvement on encryption process is 65.386%. The only disadvantage of this method is that it requires larger memory to store 4 sboxes and 2 polynomial matrices in the form of arrays for mapping. [15].

E. International Data Encryption Algorithm (IDEA)

IDEA algorithm works on block cipher. It is a minor modification of the cipher DES. It encrypts a 64-bit plaintext block into a cipher text block of 64-bit using key length 128 bit. The generator sub-key takes the 128-bit key and produces 52 sub keys (K1, K2, K3, K4, ----- K52), each of length 16 bits. The algorithm has 17 rounds, eight are even number rounds and nine are odd number rounds in those rounds. The even round takes 2 sub keys, and four sub keys take up odd number rounds. The 64-bit plain text is split into 4 equal parts of 16-bit blocks and is ready for round 1 input. The round 1output is used as round 2 input. Likewise, the round 2 output is used as round 3 input, and so on. IDEA is one of the ciphers which encrypts the information into an unreadable format and sends it over the web [11].

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

F. ATTACKS IN ATTACKS SECTION

1) Key Space and Key Sensitivity

First, the key space of an encryption algorithm should be appropriate. Thus, to test the key sensitivity, we checked the number of bit change rate (NBCR) [16]. The NBCRs of the two images B1 and B2 are defined as

$$NBCR(B_1, B_2) = \frac{ham(B_1, B_2)}{T_b}$$

Where ham (B_1, B_2) indicates the Hamming distance between B_1 and B_2, whereas Tb is the overall number of bits from B_1 or B_2. If the acquired NBCR is near to 50%, then B_1 and B_2 are entirely dissimilar images, with no relationship [16].

K_1 = {'00' '01' '02' '03' '04' '05' '06' '07''08' '09' '0a' '0b' '0c' '0d' '0e' '0f'}.

For the key sensitivity of the proposed algorithm, our experiments were designed as follows:

1st: Alter one bit of K1 to obtain K2.

2nd: Using K_1 and K_2, encrypt the plain-image P and generate two cipher-images C_1 and C_2. Then, compute their NBCR.

3rd: Decrypt the particular cipher-image C_1 by using K_1 and K_2 to get two decrypted images D_1 andD_2. Then, compute the NBCR.

In this proposed algorithm apply key space and key sensitivity attack and achieve NBCR Rate around 58%.

2) Differential Attack

Usually, a cracker performs a little amendment to the pixels of the plain image and then uses the same encryption approach to encrypt similar images. With this approach, try to find the association between a plain image and an encrypted image. To check the robustness of proposed method against differential attacks, employed the number of pixels change rate (NPCR) and unified average changing intensity (UACI) [16] on image and achieve NPCR rate 0.9998 and UACI 0.4821.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

3) **Known and Chosen Plain Text Analysis**

Generally, there are four types of cryptanalysis attacks which can be performed to break an image encryption algorithm: chosen-plain text attack, chosen-cipher text attack, known-plain text attack, and cipher text-only attack. The cryptanalysis method where the attacker picks certain plain text to obtain the related cipher text is called chosen-plain text attack. By probing the plain text and the related cipher text, they can attempt to deduce some valuable encrypted information. Finally, by means of that information, they can try to convalesce the actual images [16]. apply Known and Chosen Plain Text Analysis on image and result see in figure 3.

4) **Robustness Against Occlusion Attack**

In image processing, the extensively used parameters to check the encryption quality are peak signal to noise ratio (PSNR) and mean square error (MSE). The PSNR and MSE values between the plain (P), decrypted (D), and ciphered images can be computed as follows:

$$PSNR = 10\,X\,log_{10}\frac{(2^L-1)^2}{MSE}(dB)$$

where L is the bit-depth of the particular image. The MSE can be defined as

$$MSE = \frac{1}{HW}\sum_{r=1}^{H}\sum_{c=1}^{W}\left[P_{(r,c)} - D_{(r,c)}\right]^2$$

A higher PSNR value indicates a smaller difference between the plain and decrypted images. If P and D are the same, their PSNR will be infinity [16].

LITERATURE REVIEW

Title	Method	Obtain
Proposed Parallel Algorithms to Encryption Image Based on Hybrid Enhancement RC5 and RSA [1]	RC5 algorithm, RSA algorithm	Good security and a good speed for encrypt / decrypt the image.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

Some Secret Sharing Algorithms for Multimedia Security [2]	Multimedia Security	Light-weight encryption algorithm for the security of multimedia data. Encryption scheme is fast, provides good security with error-tolerance and adds very less overhead on the compression of the multimedia which most of the real-time multimedia applications
Performance Analysis of Elliptic Curves for Real Time Video Encryption [3]	ECC Security	They have analyzed the performance of encrypted real-time video streams using 18 ECC curves. They have considered the encryption and decryption time of all curves. We have also observed that the initial video data rate is high if we encrypt the video stream using ECC curves with smaller key size.
Video Encryption by Using Visual Cryptography Based on Wang's Scheme [4]	Cryptography	Time to Encode and decode depends on the number of frames and frame size. The more the number of frames, the longer the encoding time. Likewise, the larger the frame size, the longer the encoding time. Decoding time is very fast compared to encoding time, because the decoding process is XOR operation between the shares only.
Modified AES Based Algorithm for MPEG Video Encryption [15]	AES, MAES	MAES gives better encryption. Modified AES takes less time to encrypt and decrypt the video than simple AES.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

Text and File Encryption Application for BlackBerry Using Cipher Feedback 8-bit Mode [6]	Cipher block encryption	The software has good compatibility with many kinds of BlackBerry devices and has good security levels.

Table 1: comparison of different method and technique

Flow Chart

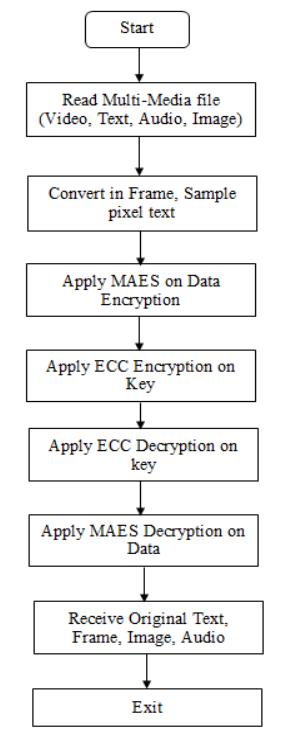


Figure 1: Flow of System

Flow Steps:

1. Read multimedia file (Audio, video, text)
2. Convert Multimedia file in preprocessing step in pixel level.
3. Apply Modified AES (MAES) on Pre-process data for Encryption.
4. To Provide Dual Layer Security apply ECC on MAES key.
5. On Receiver side For the decryption process Apply ECC decryption on cipher text.
6. Again, apply MAES Decryption on data to retrieve original content.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

7. After retrieving original content rearrange it as per original data (text, audio, and video).

ATTACK PREVENTION

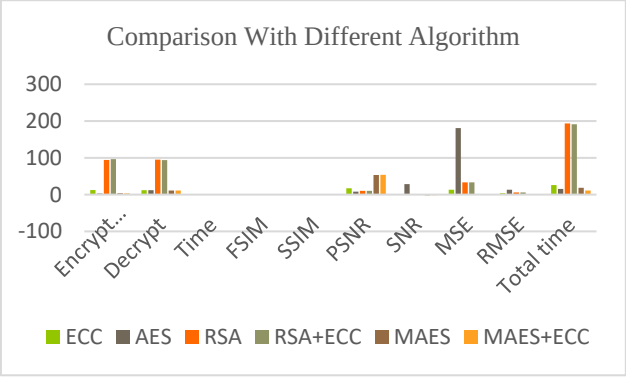
The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are two most common quantities used to evaluate the strength of image encryption algorithms/ciphers with respect to differential attacks.NPCR/UACI represent robustness against different attacks like fliplr and flipud and also random noise.so apply NPCR/UACI on proposed algorithm gives high value of NPCR and Less value of UACI result as compared to existing system so it prove that combination of MAES +ECC provide advance dual layer security against attack. Because of dual layer security of data reverse engineering also not possible because of using ECC is Perfect Forward Secrecy (PFS) and MAES provide robustness of design with less time complexity.

Result Analysis

Table: 1 Comparison with different algorithms

	ECC	AES	RSA	RSA+ECC	MAES	MAES+ECC
Encrypt time	12.41	2.64	94.04	96.47	3.61	2.3
Decrypt Time	11.91	11.96	95.15	93.92	11.22	4.1
FSIM	0.899	0.030	0.79	0.80	0.82	NAN
SSIM	0.79	0.55	0.87	0.81	0.899	1
PSNR	17.16	8.12	10.09	10.09	53.36	INF
SNR	0.047	28.43	0.039	0.039	-2.02	0
MSE	13.42	180.63	33.25	33.25	0.615	0
RMSE	3.664	13.44	5.76	5.76	0.784	0
Total time	26.0015	15.47	193.402	191.275	18.512	6.41

Figure 1: comparison with different algorithm



Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

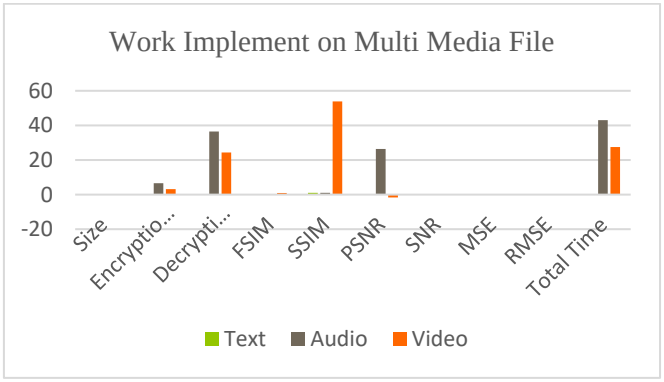
Table:2 Proposed work implemented on Multi-Media files

Parameters	Text	Audio	Video
Size	1 kb	30kb	10.355 kb
Encryption time	0.466650	13.03	49.66
Decryption Time	0.544511	8.24	17.50
FSIM	NAN	NAN	NAN
SSIM	1	1	1
PSNR	INF	INF	INF
SNR	0	0	0
MSE	0	0	0
RMSE	0	0	0
Total Time	1.011	21.27	67.166

Figure 2: Proposed work implemented on Multi-Media files

Images	NPCR	UACI
All White	0.9998	0.4166
Cipher white	0.9998	0.4163
Full Black	0.9999	1.000
Cipher Black	0.9998	0.9994

Figure 3: Known and Chosen Plain Text Implemented on Multi-Media files



Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

CONCLUSION

This paper proposed a new method of dual layer security on multimedia files. Algorithms vary in terms of parameter which includes encryption time, and decryption time, PSNR, FSIM, SSIM, and SNR and also Proposed Algorithm Provide Robust against Key Space and Key Sensitivity, Differential Attack, Known and Chosen Plain Text Analysis, Robustness against Occlusion Attack. The comparison table of MAES and ECC shows that Hybrid approach takes less time for encryption as well as decryption and improves other parameters and also Revers Engineering is not possible because of Random key generator so it increase security of proposed system as Compared to Existing. So, it can be concluded that hybrid approach is more efficient than other cryptography method. In Future work on other large databases.

References

[1] Khaled Ali Hussein, Taha Basil Kareem, "Proposed Parallel Algorithms to Encryption Image Based on Hybrid Enhancement RC5 and RSA", IEEE, 2019.

[2] Nilanjan Sen, Ram Dantu, Jagannadh Vempati, Mark Thompson, "Performance Analysis ofElliptic Curves for Realtime Video Encryption", IEEE - National Cyber Summit Research Track, 2018.

[3] Rinaldi Munir, Harlili, "Video Encryption by Using Visual Cryptography Based on Wang's Scheme", IEEE , 2018.

[4] Ms. Pooja Deshmukh, Ms. Vaishali Kolhe, "Modified AES Based Algorithm for MPEG Video Encryption", IEEE, 2014.

[5] Matthew Wangsadiredja, Dr. Ir. Rinaldi Munir, M.T, "Text and File Encryption Application for BlackBerry Using Cipher Feedback 8-bit Mode", IEEE, 2011.

[6] Xin Zhou, Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", IEEE- International Forum on Strategic Technology, 2011.

[7] Dr. K.L. Vasundhara *, Y. V. S. Sai Pragathi**, Y. Sai Krishna Vaideek ***., "A Comparative Study of RSA and ECC ", IJERA, ISSN: 2248-9622, Vol. 8, Issue 1, (Part -I) January 2018.

[8] Luminiţa SCRIPCARIU and Mircea-Daniel FRUNZĂ, "Modified Advanced Encryption Standard", IEEE, 2012.

[9] Flevina Jonese D'souza, Dakshata Panchal, "Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach", IEEE, 2017.

[10] Prajwal VS and Prema KV, "User Defined Encryption Procedure For IDEA Algorithm", IEEE, 2018.

[11] Sridhar C. Iyer1, R.R.Sedamkar2, Shiwani Gupta, "An Efficient Multimedia Encryption using Hybrid Crypto Approaches", IJRTER, ISSN: 2455-1457, 2016.

[12] Md. Khalid Imam Rahmani, Mr.Amit Kumar Goyal Manisha Mudgal," Study of Cryptography and Steganography System" , IJECS, Volume 4 Issue 8 Aug 2015.

[13] K. Kalaivani and B. R. Sivakumar, "Survey on Multimedia Data Security", International Journal of Modeling and Optimization, Vol. 2, No. 1, February 2012.

[14] Rashmin Tanna et al., International Journal of Research in Engineering, IT and Social Sciences, ISSN 2250-0588, Impact Factor: 6.452, Volume 08 Issue 04, April 2018, Page 65-68.

[15] Khushbu Khalid Butt, Guohui Li , Sajid Khan and Sohaib Manzoor, "Fast and Efficient Image Encryption Algorithm Based on Modular Addition and SPD", MDPI, 2020.