Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES) – An International Journal
ISSN: 2566-932X, Vol. 2, Issue 1, April 2018

A Cryptographic Algorithm Combining Advanced Encryption Standard and Visual Cryptography

Aakanksha N, Aditi G S V, Amulya S, Likith K C
Department of Telecommunications, Bangalore Institute of Technology, Bangalore, India

Abstract: With the increased usage of Internet and other online services, most of our personal information is now available online. If such sensitive data falls into wrong hands, it can be misused. Thus, in order to avoid such mishaps, a highly secure cryptographic technique becomes a major requirement. This paper deals with one such algorithm where the advantages of Advanced Encryption (AES) and Visual Cryptography (VC) are combined to make the existing cryptographic algorithm more efficient. The AES algorithm has four steps involved to encrypt or decrypt: AddRound-key, Sub-bytes, Shift rows, and Mix columns. In the Mix columns approach, the area, power and speed need to be conserved to increase efficiency and to execute all steps of the AES judiciously. Additionally, we decrease transmission bandwidth by using a modern algorithm in VC. Furthermore, we aim to achieve the combination of both the algorithms. These intentions are brought about by using ModelSim and Xilinx software as well as the Spartan-3E FPGA kit. In conclusion, our paper aims to put forth a merging algorithm which helps the masses to have secure data.

Keywords: Advanced Encryption Standard (AES); Visual Cryptography (VC)

I. INTRODUCTION

The information to be communicated be over internet or stored are exposed to various security issues such as cyber-attacks, organized crimes, misusage of the information by intruders and other network based attacks, hence it is necessary to protect such data and resources to guarantee confidentiality, authenticity and integrity of such data. These security functions are often based on cryptographic algorithms, which occupy processing power, large area and also increases power and energy consumption [3].

One such cryptographic algorithm is AES which is a symmetric block cipher which operates on fixed number of bytes. It is a secret key encryption algorithm. In AES same operations are performed multiple times on a fixed number of bytes. The operations are AddRound Key, SubBytes, ShiftRows and MixColumn[6]. AES supports multiple security levels by providing different key sizes and increases security. In a recent study in 2016 it was found that AES was hack able within 3 seconds hence there was necessity to strengthen this technique.

In this paper, we will be designing a highly secure encryption technique by combining AES and VC. VC is a type of secret sharing scheme where the secret to be shared is a binary image, which is cryptographically encoded into 'n' shares of random binary patterns and distributed among participants. No participant will know the share of other participant. The secret is decoded by superimposing k or more shares together. The secret cannot be decoded with K-1 or fewer shares[2]. VC has many applications such as biometric privacy, watermarking, visual authentication etc.

II. RELATED WORK

In a literature survey, a number of works have been reported for cryptographic techniques [1], [2]. The existing work is described in the following manner:

Of late, users' personal information need not be stored in the users' personal data storage, but it may be stored in remote servers. Cloud computing is an integral piece of technology for sharing resources due to its flexibility, scalability and reduced cost factors. With the advent of cloud computing, data security is paramount in ensuring confidentiality, integrity and authenticity in data transmission and storage. Contents such as text, images, videos etc., need to be highly encrypted without loss in information during the process. [1]

'A Novel Cryptographic Encryption Technique for Securing Digital Images in the Cloud using AES and RGB pixel displacement' by Quist-Aphetsi Kester et. al [1] proposed an image encryption process which is a combination of AES and an RGB cryptographic technique. Here, they generated a secret shared key using the AES-256 algorithm. Then, they shifted and displaced the numerical pixel values of the plain image and the RGB values were interchanged and shuffled using the previously generated key. They concluded that there was no loss of pixel values or pixel expansion, i.e., the pixel attributes remained unchanged.

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. User authentication is an important process in the area of security. Most of the existing user authentication schemes use expensive cryptographic algorithms and cannot successfully prevent brute force and dictionary attacks. Visual cryptography is a secret sharing technique that requires less computation. [2]

'User Authentication using Visual Cryptography' by Praveen Kumar. P et. al [2] designed a user authentication scheme using VC. They have provided insight into user authentication scenario with two parties, where one of the two shares is fixed (pre-share) and the other (authentication share) can be changed to share any secret. A major drawback is the difficulty to correlate multiple authentication shares. They state that this can be overcome by a protocol in which the user registers to a server and then achieves mutual authentication between the user and the server. They concluded that their scheme creates a secure communication channel which is not required to be previously established between the user and the server.

III. PROPOSED SYSTEM

In this paper, a hybrid approach in the encryption and decryption of the message using AES and Visual cryptography was adopted. Our main aim is to increase the efficiency of Mix column step of AES with respect to area. Second main aspect is to use VC such that it requires minimum bandwidth. The ideology of combining two major encryption techniques that is AES and VC is proved to be very innovative and unique.

A. Input data

Input text data is procured from the user and 128-bit AES is performed over the same.

B. AES

AES consists of following steps:

a) Add Round Key
b) Sub-bytes
c) Shift rows
d) Mixed Columns

In add round key step, each element of the input matrix undergoes XOR operation with a key generated. The same has been demonstrated in Fig 1.

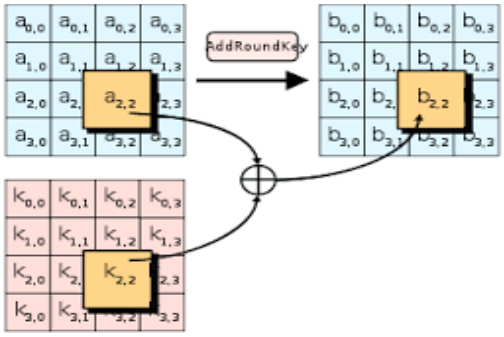

Fig 1. Add round key

In cryptography, an S-box is a basic component which performs substitution. Each element from output of AddRoundKey step is replaced by its equivalent value in S-box.

In this process, the elements of matrix are shifted left. First row is unaffected whereas second, third and fourth row is shifted left by count of one, two and three respectively as shown in Fig 2.

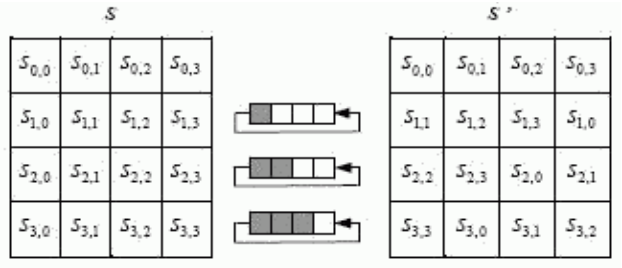

Fig 2. Shift rows

In mixed column step, the matrix is multiplied with a predefined key over Galois field. The multiplication is performed one column at a time (4 bytes). Each value in the column is eventually multiplied against every value of the matrix (16 total multiplications). The results of these multiplications are XORed together to produce only 4 result bytes for the next state. Therefore 4 bytes input, 16 multiplications 12 XORs and 4 bytes output. The multiplication is performed one matrix row at a time against each value of a state column. Mix column is performed using Look Up Tables' Approach as explained in [1].

The pre-defined key used in encryption is

$$\begin{Bmatrix} 2\,3\,1\,1 \\ 1\,2\,3\,1 \\ 1\,1\,2\,3 \\ 3\,1\,1\,2 \end{Bmatrix} \quad (1)$$

C. Visual Cryptography

The elements from the encrypted data is divided into two shares by randomly picking elements and putting them into the shares

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

1			4		2	3	
	6	7		5			8
		11	12	9	10		
13			16		14	15	

Share 1 Share 2

Fig 3. Visual Cryptography Process

E Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	01	03	05	0F	11	33	55	FF	1A	2E	72	96	A1	F8	13	35
1	5F	E1	38	48	D8	73	95	A4	F7	02	06	0A	1E	22	66	AA
2	E5	34	5C	E4	37	59	EB	26	6A	BE	D9	70	90	AB	E6	31
3	53	F5	04	0C	14	3C	44	CC	4F	D1	68	B8	D3	6E	B2	CD
4	4C	D4	67	A9	E0	3B	4D	D7	62	A6	F1	08	18	28	78	88
5	83	9E	B9	D0	6B	BD	DC	7F	81	98	B3	CE	49	DB	76	9A
6	B5	C4	57	F9	10	30	50	F0	0B	1D	27	69	BB	D6	61	A3
7	FE	19	2B	7D	87	92	AD	EC	2F	71	93	AE	E9	20	60	A0
8	FB	16	3A	4E	D2	6D	B7	C2	5D	E7	32	56	FA	15	3F	41
9	C3	5E	E2	3D	47	C9	40	C0	5B	ED	2C	74	9C	BF	DA	75
A	9F	BA	D5	64	AC	EF	2A	7E	82	9D	BC	DF	7A	8E	89	80
B	9B	B6	C1	58	E8	23	65	AF	EA	25	6F	B1	C8	43	C5	54
C	FC	1F	21	63	A5	F4	07	09	1B	2D	77	99	B0	CB	46	CA
D	45	CF	4A	DE	79	8B	86	91	A8	E3	3E	42	C6	51	F3	0E
E	12	36	5A	EE	29	7B	8D	8C	8F	8A	85	94	A7	F2	0D	17
F	39	4B	DD	7C	84	97	A2	FD	1C	24	6C	B4	C7	52	F6	01

L Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0		00	19	01	32	02	1A	C6	4B	C7	1B	68	33	EE	DF	03
1	64	04	E0	0E	34	8D	81	EF	4C	71	08	C8	F8	69	1C	C1
2	7D	C2	1D	B5	F9	B9	27	6A	4D	E4	A6	72	9A	C9	09	78
3	65	2F	8A	05	21	0F	E1	24	12	F0	82	45	35	93	DA	8E
4	96	8F	DB	BD	36	D0	CE	94	13	5C	D2	F1	40	46	83	38
5	66	DD	FD	30	BF	06	8B	62	B3	25	E2	98	22	88	91	10
6	7E	6E	48	C3	A3	B6	1E	42	3A	6B	28	54	FA	85	3D	BA
7	2B	79	0A	15	9B	9F	5E	CA	4E	D4	AC	E5	F3	73	A7	57
8	AF	58	A8	50	F4	EA	D6	74	4F	AE	E9	D5	E7	E6	AD	E8
9	2C	D7	75	7A	EB	16	0B	F5	59	CB	5F	B0	9C	A9	51	A0
A	7F	0C	F6	6F	17	C4	49	EC	D8	43	1F	2D	A4	76	7B	B7
B	CC	BB	3E	5A	FB	60	B1	86	3B	52	A1	6C	AA	55	29	9D
C	97	B2	87	90	61	BE	DC	FC	BC	95	CF	CD	37	3F	5B	D1
D	53	39	84	3C	41	A2	6D	47	14	2A	9E	5D	56	F2	D3	AB
E	44	11	92	D9	23	20	2E	89	B4	7C	B8	26	77	99	E3	A5
F	67	4A	ED	DE	C5	31	FE	18	0D	63	8C	80	C0	F7	70	07

Fig 4. E-Table and L-Table for Mix Column

In decryption process, the steps in encryption are reversed by using different key for Add round key. Inverse S-Box is used for sub-bytes and the rows are shifted right in shift rows. The 4x4 matrix obtained is mapped to the alphabets and numbers to recover the original information.

IV. CONCLUSION

Visual Cryptography is used to split the image into number of shares. The traditional method of VC[4] will replace every pixel with pair of pixels in each share. This doubles the size of image resulting in pixel expansion. In the proposed algorithm each pixel of the original image has only one pixel in one of the shares. This saves the bandwidth of the network.

REFERENCES

[1] S. R. Rupanagudi et al., "Optimized area and speed architectures for the mix column operation of the advanced encryption standard," 2017 International Conference on Robotics, Automation and Sciences (ICORAS), Melaka, 2017, pp. 1-5.

[2] Quist-Aphetsi Kester, Laurent Nana and Anca Christine Pascu. "A Novel Cryptographic Encryption Technique for Securing Digital Images in the Cloud using AES and RGB pixel displacement", 2013 European Modelling Symposim.

[3] Praveen Kumar. P and Sabitha. S, "User Authentication using Visual Cryptography", 2015 international Conference on Control, Communication And Computing India (ICCC), 19-21 November.

[4] Duy-Heiu Bui, Student Member, IEEE. Diego Puschini, Simone Bacles-Min, Edith Beigne, Senior Member, IEEE, and Xuan-Tu Trang, Senior Member IEEE. "AES Datapath Optimization Strategies for Low-power and Low-energy Multi-security level Internet-of-Things application", IEEE Transactions on VSLI Systems, VOL.25, NO.12, December2017.

[5] Ran-Zan Wang and Shuo-Fang Hsu, "Tagged Visual Cryptography", IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 11, NOVEMBER 2011 627

[6] R.M. Shiny, P. Jayalakshmi, A. Rajakrishnammal, T. Sivaprabha, Abrami. R, "An Efficient Tagged Visual Cryptography for Colour Images", IEEE International Conference on Computational Intelligence and Computing Research, (ICCIC), Agni College of Technology, Thalambur, Chennai, 15 to 17 December 2016.

[7] William Stallings, "Cryptography and Network Security", third edition, Pearson Education, Delhi India, 2003, ch. 5, pp 139-196.

[8] AddRoundKey Step (2012) [Online]. Available: https://www.aescryptography.blogspot.in/2012/05/addroundkey-step.html

[9] Shift Rows in AES [Online]. - https://lapastina.wordpress.com/tag/aes/

[10] E-table and L-table [Online] - https://crypto.stackexchange.com/questions/19986/aes-mix-column-stage