INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue4)

Available online at: www.Ijariit.com

Design of Low Area and Secure Encryption System Using Combined Watermarking and Mix-Column Approach

Swati Sharma*
Dept. of ECE
Sambhram Institute of Technology
Bengaluru, India
sharmasankhyan1990@gmail.com

Dr.M.Levy
Dept. of ECE
Sambhram Institute of Technology
Bengaluru, India
levy_young@yahoo.com

Abstract*— Lately, the significance of security in the data innovation has expanded fundamentally. This paper shows another proficient design for rapid and low range propelled encryption standard calculation utilizing part strategy. The proposed engineering is actualized utilizing Field Programmable Gate Array.

Keywords*— Advanced Encryption Standard(AES), Mix-column, LUT(Look-up table) approach, GF (Galois Field), Splitting method.

I. INTRODUCTION

The Advanced Encryption Standard (AES) is formal encryption strategy which was embraced by the National Institute of Standards and Technology of the US Government, and is acknowledged around the world. The National Institute of Standards and Technology (NIST), a branch of the US government, began a procedure to have a substitution for the Data Encryption Standard (DES). It was perceived that DES was not secure due to progresses in PC handling power. The objective of NIST was to characterize a swap for DES that could be utilized for non-military data and security applications by US government organizations.

The AES calculation itself is not a PC project or PC source code. It is a numerical portrayal of a procedure of darkening information. Various individuals have made source code usage of AES encryption; including the first authors.AES encryption utilizes a solitary key as a part of the encryption procedure. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) long. The term 128-piece encryption alludes to the utilization of a 128-piece encryption key. With AES both the encryption and the unscrambling are performed utilizing the same key. This is known as a symmetric encryption calculation. Encryption calculations that utilization two distinctive keys, an open and a private key, are called deviated encryption calculations [1].

An encryption key is basically a double string of information utilized as a part of the encryption procedure. Since the same encryption key is utilized to scramble and unscramble information, it is vital to keep the encryption key a mystery and to utilize keys that are difficult to figure. Some keys are created by programming utilized for this particular errand. Another technique is to get a key from a pass expression. Great encryption frameworks never utilize a pass expression alone as an encryption key. AES was characterized with some fundamental necessities which requires 128-piece squares acknowledges keys of size 128, 192 and 256 bits (128 bits are adequate to oppose comprehensive key hunt) likewise it has no scholastic shortcoming more

terrible than thorough key inquiry, so it ought to be as quick as 3DES (AES ended up being much speedier than 3DES in programming, around 5 to 10 times quicker).

The way toward encoding the plaintext into figure content is called Encryption and opposite the way toward deciphering figures content to plaintext is called Decryption. This should be possible by two methods symmetric-key cryptography and uneven key cryptography. Symmetric key cryptography includes the use of the same key for encryption and decoding. In any case, the Asymmetric key cryptography includes the use of one key for encryption and another, distinctive key for decoding. Mystery key cryptography incorporates DES, AES, 3DES, IDEA, Blowfish calculations and so on and open key cryptography incorporates RSA and Digital Signature [3][4]. For every calculation there are two key angles utilized: Algorithm sort (characterize size of plain content ought to be encoded per step) and calculation mode (characterize cryptographic Algorithm mode). Calculation mode is a blend of a progression of the essential calculation and some square figure and some criticism from past strides.

There are a few encryption benchmarks amongst which DES, 3-DES and AES are talked about underneath:

Information Encryption Standard: DES is a piece figure. It encodes the information in a square of 64 bits. It produces 64 bit figure content. The key length is 56 bits. At first the key comprises of 64 bits. The bit position 8, 16, 24, 32,40,48,56, 64 disposed of from the key length [5].DES depends on two principal properties of cryptography: Substitution (disarray) and transposition (Diffusion). DES comprises of 16 stages, each of which called as a Round [2].

Triple DES: Triple DES will be DES - three times. It comes in two structures: One that utilizations three keys, and other that utilizations two keys. The plain content piece An is initially encoded with a key B1, then scrambled with second key B2, lastly with third key B3, where B1, B2 and B3 are not quite the same as each other. To decode the figure content C and get the plain content, we have to play out the operation A= DB3 (DB2 (DB1(C))) [2]. Alanazi et al. has done the near investigation of three Encryption Algorithms (DES, 3DES and AES) inside nine elements, for example, Key Length, Cipher Type, Block Size, Security, Possible Keys, Possible ASCII printable character keys and Time required to check all conceivable keys at 50 billion keys every second and so forth. Study demonstrates that AES is superior to anything DES and 3-DES [8].

Since security is the primary point of view now-a-days so there is a need of some propelled techniques for encryption and decoding. We have talk about the different techniques for encryption i.e. DES, 2-DES, 3-DES and AES, amongst which AES gives better security and is 5 to 10 times quicker than 3-DES[9]. AES is performed utilizing LUT strategy.

II.LITERATURE SURVEY

Seth et al. have done the relative examination of three calculations; RSA, DES and AES while considering certain parameters, for example, calculation time, memory utilization and yield byte. These parameters are the real issue of worry in any Encryption Algorithm. Trial results demonstrate that DES calculation expends minimum encryption time and AES calculation has slightest memory utilization while encryption time contrast is exceptionally minor if there should be an occurrence of AES and DES calculation. RSA expend longest encryption time and memory use is additionally high however yield byte is slightest if there should arise an occurrence of RSA calculation.

Abdul. Elminaam et al. learned about the execution of Symmetric Encryption Algorithms. This paper gives assessment of six of the most widely recognized encryption calculations: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. A correlation has been led at various settings for every calculation, for example, diverse sizes of information squares, distinctive information sorts, battery power utilization, diverse key size lastly encryption/decoding speed. Exploratory re-enactment indicates taking after results. There is no noteworthy distinction when the outcomes are shown either in hexadecimal base encoding or in base 64 encoding. If there should arise an occurrence of changing parcel size, it was found that RC6 requires less time than all calculations aside from Blowfish. If there should be an occurrence of changing information sort, for example, picture rather than content, it was found that RC2, RC6 and Blowfish has hindrance over different calculations as far as time utilization. Likewise, 3DES still has low execution contrasted with calculation DES. At long last - on account of changing key size (conceivable just in AES and RC6 calculations) it can be seen that higher key size prompts clear change in the battery and time utilization.

Alanazi et al. has done the similar investigation of three Encryption Algorithms (DES, 3DES and AES) inside nine components, for example, Key Length, Cipher Type, Block Size, Security, Possible Keys, Possible ASCII printable character

keys and Time required to check all conceivable keys at 50 billion keys every second and so forth. Study demonstrates that AES is superior to anything DES and 3DES.

III.METHODOLOGY

Proposed method: Watermarking along with splitting method

Bit-planar Method for watermarking: In bit-planar technique message can be any coded or straight orchestrate of bits or a picture. For this anticipate two RGB pictures are viewed as, one is mystery key picture and another is spread picture. Both the RGB pictures are changed over to greyscale pictures utilizing MATLAB. At that point most critical bit(MSB) of spread Image and slightest huge bit(LSB) of mystery key picture is taken and consolidated together to get a watermarked picture. The stream of bit-planar technique is appeared in the figure underneath: Flowchart of Bit-planar Method for watermarking:

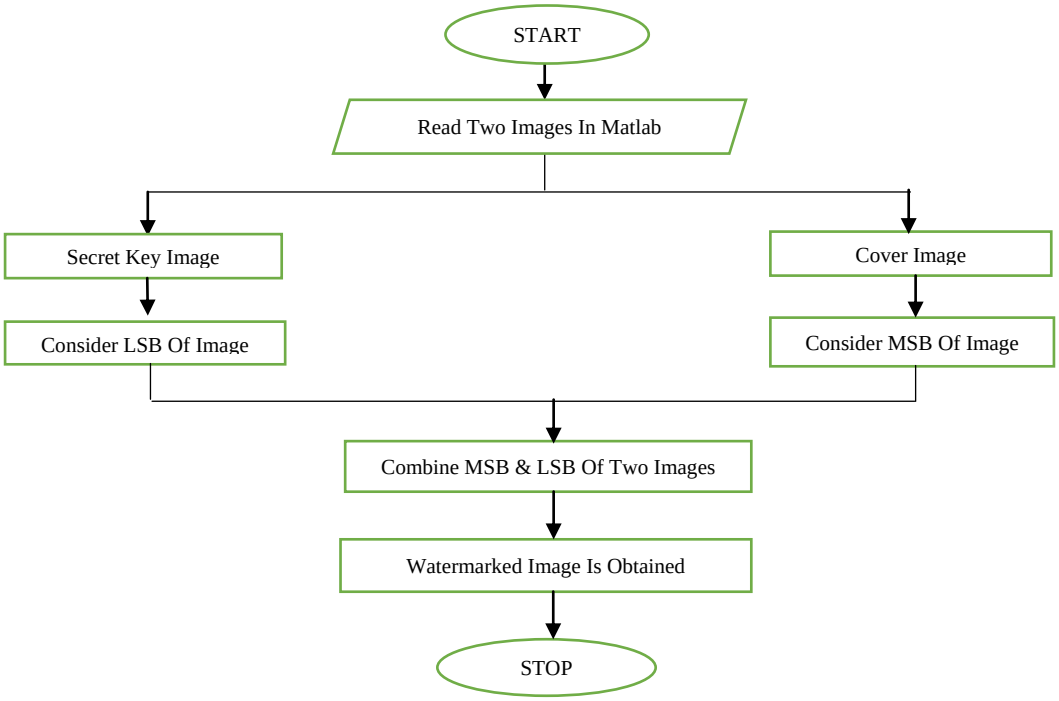
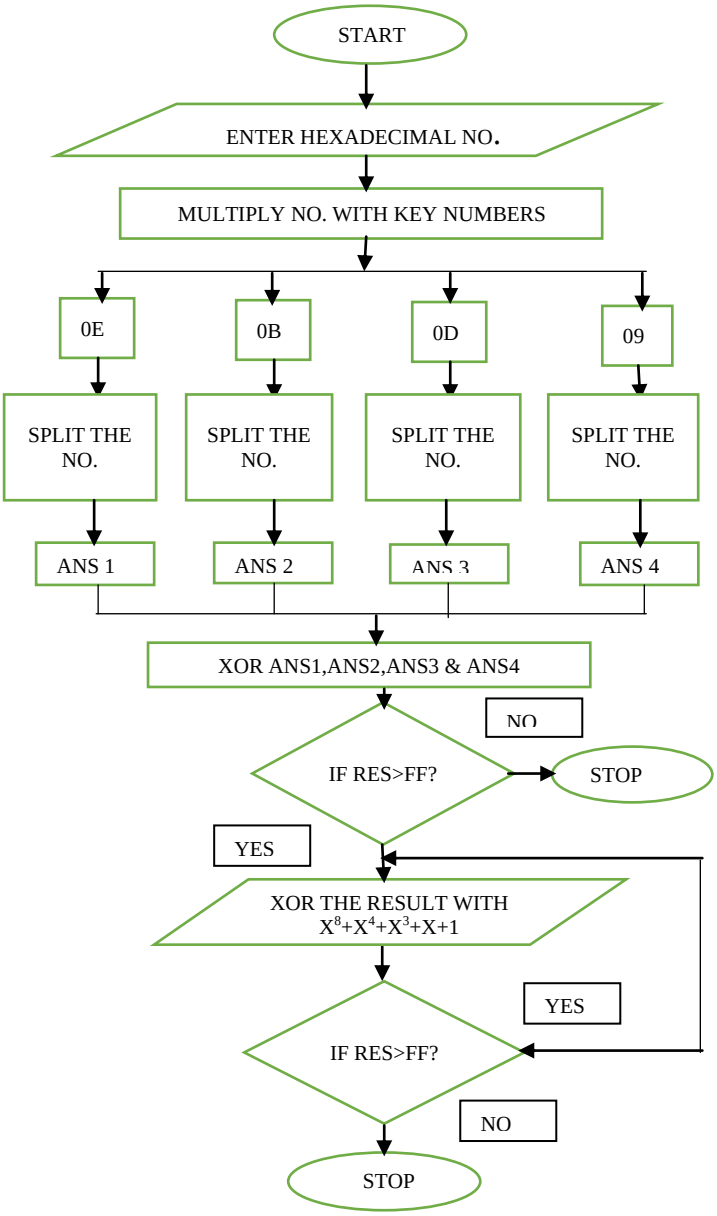


Fig.1 Flowchart showing LUT approach

Splitting Method: The after-effects of the blend segments operation are computed utilizing GF (2^8) operations. Every component of GF (2^8) is a polynomial of degree 7 with coefficients in GF(2) (or equally Z^2). Along these lines, the coefficients of every term of the polynomial can take the worth 0 or 1. Given that there are 8 terms in a component of GF (2^8), a component can be spoken to by bit string of length 8, where every piece speaks to a coefficient.

We will utilize the slightest critical piece to speak to the steady of the polynomial, and going from right to left, speak to the coefficient of xi by the bits to one side of the minimum noteworthy piece.

Flowchart of splitting method:



.Fig. 2 Flowchart of Steps Involved in Splitting Method

Multiplication of two components in GF (2^8) requires more work. The multiplication of two components of Z^2 is reenacted with an AND entryway. Augmentation in GF (2^8) can then be refined by first increasing every term of the second polynomial with the greater part of the terms of the principal polynomial. Each of these items ought to be included. In the event that the level of the new polynomial is more noteworthy than 7, then it must be diminished modulo some irreducible polynomial. On account of AES, the irreducible polynomial is $x^8 + x^4 + x^3 + x + 1$[10].

IV.RESULTS AND CONCLUSIONS

The look-up table methodology and our proposed design was executed on Spartan 3e arrangement of FPGA and the combination results for the same is as demonstrated as follows. It is obviously watched that the part technique is 4 ns quicker than LUT approach. Likewise part technique takes just 2% of the zone on the chip though LUT approach take 20% of the region when actualized on a Spartan 3e arrangement of FPGA.

TABLE 1

Algorithm	**Time Taken(ns)**	**Area occupancy (%)**	**Power Consumed (Watts)**
LUT Approach(Existing Method)	13.941	21% area of the chip	0.032
Splitting Method (Proposed Method)	9.812	3% area of the chip	0.031

ACKNOWLEDGMENT

I would like to articulate deep gratitude to my project guide Dr. M. Levy and co-guide Prof. Pranita Palsapure who have always been my motivation for carrying out the paperwork. I express my deep sense of gratitude to my family members who have always been a great source of inspiration.

REFERENCES

[1] Introduction toAES encryption by townsend security.

[2] Sombir Singh, *"Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques"*, International Journal of Advanced Research in Computer Science and Software Engineering,Vol 3, Issue 6, June-2013

[3] Atul Kahte, *"Cryptography and Network Security"*,Tata Mcgraw Hill, 2007.

[4] Wuling Ren, *"A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication"*,Second International Conference on Modeling", Simulation and Visualization Methods (WMSVM), 2010.

[5] Gurpreet Singh, *"A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security",*International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013

[6] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, *"New Comparative Study Between DES, 3DES and AES within Nine Factors"*, Journal Of Computing, Volume 2, ISSUE 3, pp. 152-157, MARCH 2010.

[7] Ambika R., CS Mala, *"FPGA implementation of AES using Vedic Mathematics"* (IJIRSE) International Journal of Innovative Research in Science & Engineering ISSN (Online) 2347-3207

[8] Hua Li Zac Friggstad *"An Efficient Architecture for the AES Mix-Columns Operation"*0-7803-8834-8/05/$20.00 ©2005 IEEE, Page -4637-4640

