Computer Science and Engineering 2012, 2(5): 63-67
DOI: 10.5923/j.computer.20120205.04

Secure Transmission of Biometric Scan Images Using Data Encryption Standards(DES) Algorithm

Ghanshyam Gaur[1,*], R. S. Meena[2]

[1]Digital Communication, University College of Engg, Rajasthan Technical University, Kota , Rajasthan, 324010, India
[2]Deptt. Of Electronics, University College of Engg, Rajasthan Technical University, Kota, Rajasthan, 324010, India
rssmeena@gmail.com

Abstract Biometric Scan Images, however, is vulnerable to unauthorized access while in storage and during transmission over a network. Unauthorized user can make a fake copy from image file from memory device or computer. Biometric Data in form of images are very confidential information of user. If they are in unauthorized hand then misuse of data may be harmful to authorized user. As in case of Unique ID each and every citizen of country have their Biometric scan images of finger, face and thumb and Iris all in original form like JPEG,JPG,GIF,PNG,BMP etc. To protect them from unauthorized access we can encrypt images so they can't be detected and used. Protection is required at very initial end so that images can be directly saved in form of encrypted image in memory device. First image will be converted into pixels. Each pixel will be converted into DataStream and stored in codebook in same order as of pixels in image. Digitized pixels will have a group of data bits and each pixels or set of pixels will be encrypted using DES algorithm. The whole Programming and design can be done in any platform like MATLAB, C, C++, Xilinx ISE 13.4 Software. The advantage of using Xilinx is that in this platform we can design a Layout of it so that finally a Chip level Solution can be provided.

Keywords Data Encryption Standards, Encryption, Decryption, S-Box, Very High Speed Logic Hardware Description Language

1. Introduction

This Image Digitization Using wavelet Transform in Matlab has been done, Image encryption implemented on Matlab. Data Encryption Standards (DES) Implemented Using VHDL. FPGA implementation has been done of DES, Xilinx
implementation has been done of DES, Pipeline and Non-pipeline effects have been measured of DES. Text Data encryption [6] Using DES have done.

So the Security of biometric scan images can be done using DES in any platform. Now we are encrypting images using DES in this design and all this is performed using verilog Hardware description language on Xilinx ISE 13.4 Design Suit software and this tool will also help in designing of layout of chip so that we can use it at industry level for making similar encryption chips at large scale.

Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. Biometric Scan Images, is vulnerable to unauthorized access while in storage and during transmission over a network. Unauthorized user can make a fake copy from image file from memory device or computer. Biometric Data in form of images are very confidential information of user. If they are in unauthorized hand then misuse of data may be harmful to authorized user. Data Encryption Standard[5][1] (DES) is a well known block cipher that has several advantages in data encryption. It gives us to reflect a high level security and better image encryption. The modification is done by adjusting the Shift Row Transformation. Detailed results in terms of security, analysis, implementation[3] are given. Experimental results verify and prove that the proposed modification to image cryptosystem is highly secure from the cryptographic viewpoint.

The Data Encryption Standard (DES) algorithm is the most widely used encryption algorithm in the world. For many years, and among many people, "secret code making" and DES have been synonymous. And despite the recent coup by the Electronic Frontier Foundation in creating a $220,000 machine to crack DES-encrypted messages, DES will live on in government and banking for years to come through a life- extending version called "triple-DES."

Data Encryption Standard (DES) encrypts and decrypts data in 64-bit blocks, using a 64-bit key (although the effective key strength is only 56 bits, as explained below). It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in

* Corresponding author:
gaurghanshyam08@gmail.com (Ghanshyam)
Published online at http://journal.sapub.org/computer

the algorithm, DES is both a block cipher and a product cipher.

DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially.

Here the theoretical Concept used is the bit pattern generated from image is changed into a new bit pattern using logic synthesis tool Data encryption standards (DES), which gives a new bit pattern (Called as encrypted bit pattern) which is different from original.

So resulting image formed by this new bit pattern will also have no resemblance of original, so we can hide our original image from unauthorized access using this image in storage in place of original. While original image is reconstruct able by decrypting this image which is possible only for the authorized user.

2. Digitization of Image

A biometric identifier known as a retinal scan is used to map the unique patterns of a person's retina.

The blood vessels within the retina absorb light more readily than the surrounding tissue and are easily identified with appropriate lighting.

A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece.

This beam of light traces a standardized path on the retina. Because retinal blood vessels are more absorbent of this light as shown in fig.1 than the rest of the eye, the amount of reflection varies during the scan. The pattern of variations is converted to computer code and stored in a database.

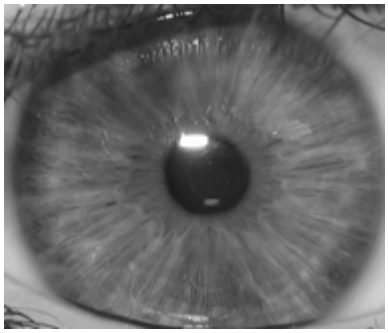

Figure 1. Image capture[9]

The fig. 1 shows a biometric iris scan used as a biometric scan data in identification of citizens.

Impressions of fingerprints may be left behind on a surface by the natural secretions of sweat from the eccrine glands that are present in friction ridge skin, or they may be made by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card as shown in fig.2 Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.

Figure 2. Right Hand Impression[10]

And also the image[8] data are in form of finger prints and thumb impressions etc. of a person, all are very confidential data for any Citizen of a country.[7]

Because on the basis of this we can access the personal data and their any professional information stored in central register of country.

2.1. Image Conversion into Digits

A trial image[2] is first converted into Pixels. Each pixel is then converted into DataStream & DataStream is saved in Code book.

The codebook contains the bit series of each pixel in the same location and this location is important because the same locations' bit series will give the same pixel so these locations should be matched when we are applying Encryption and Decryption.

The DES is applied to each pixel or group of pixels' DataStream taken from codebook.

Resultant encrypted image is stored in Central Server.

For Decryption DES is applied in reverse order to encrypted result & then each pixel is arranged in same order to get original image.[2]

2.2. Image Datastream

The 8-bit transformation of image[4] will have 256 pixels so we have 256*8 bits, but we know that the DES implementation will require 64 bits for this, so we will apply the DES to the group of pixels so for 64 bits' group we take 8 pixels at a time.

And the DES loop will be Re-apply to another 8 pixels so 64* 32 bits will covers in 32 loops.

The bits no. D (1) to D (32) will first processed and then D (33)

To D (64) and so on up to D (2013) to D (2048) bit in 32 loops.

3. Implementation of DES

The Data Encryption Standard (DES)[5][6][1] is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally. It is based on a symmetric-key algorithm that uses a 56-bit key.

3.1. Data Encryption Standards

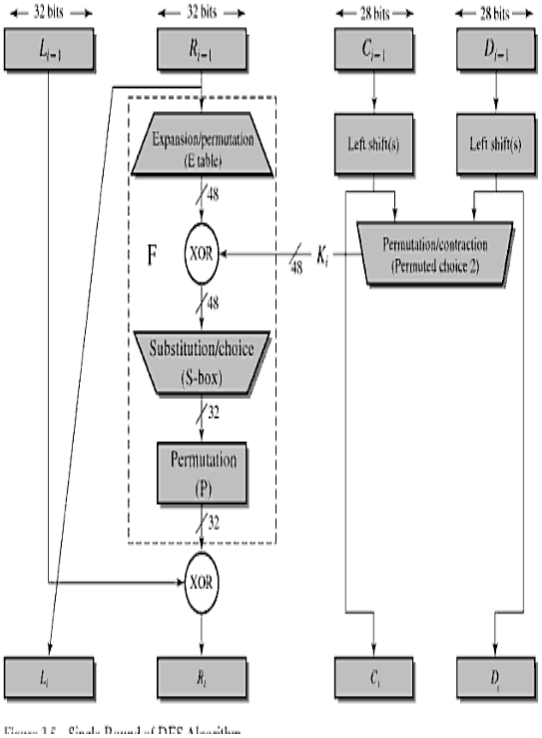

Figure 3. DES algorithm[11]

DES[5] is the archetypal block cipher an algorithm that 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. In the case of DES, the block size is 64 bits as in fig.3 used. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is never quoted as such. Every 8th bit of the selected key is discarded, that is, positions 8, 16, 24, 32, 40, 48, 56, 64 are removed from the 64 bit key leaving behind only the 56 bit key. Fig. 3 shows the whole DES algorithm.

Image encryption technique is a new encryption technique for images, which is an efficient way to deal with the intractable problem of fast and highly secure image encryption. DES encryption and a combination of image encryption algorithm, and simulate these algorithms, through analysis of the algorithm to find the gaps. And on this basis, the algorithm has been improved. Firstly, new encryption[1] scheme uses the logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES[5], displays they respective merit. Theoretical analysis and the simulation indicate that this plan has the high starting value sensitivity, and enjoys high security and the encryption speed. In addition it also keeps the neighboring RGB relevance close to zero. The algorithm can be used in the actual image encryption

3.2. S-box

The S-boxes[1] are somewhat different from the other permutations. While all the others are set up according to "bit x goes to bit y", the input bits can be viewed differently for the S-boxes. If the input is {i1,i2,i3,i4,i5,i6} then the two-bit number {i1,i6} and the the four-bit number {i2,i3,i4,i5} are used as indices to the table. As shown in fig. 4 For the 48-bit word {i1, i2 … i48}, the word {i1 … i6} is sent to S-box 1, the word {i7 … i12} to S-box 2, etc. The output of S-box 1, {o1 … o4}, that of S-box 2, {o5 … o8} etc. are concatenated to form the output of 32 bits resulting from 4 bits from 8 S-boxes as in the end of fig. 4

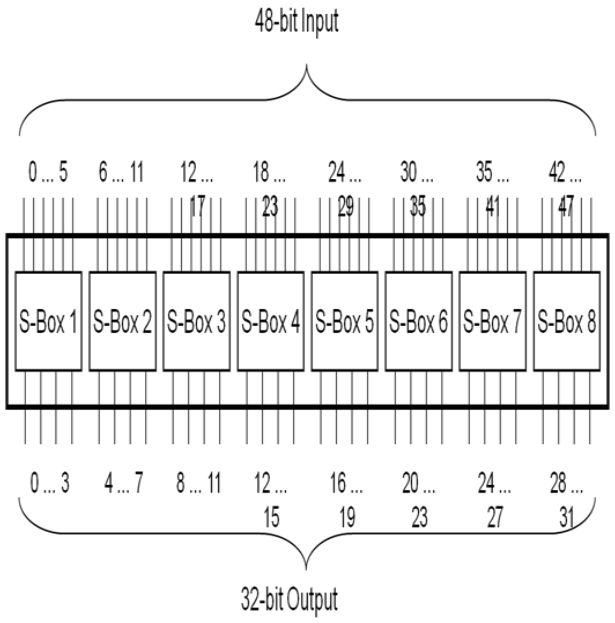

Figure 4. The 8 DES S-Boxes[11]

3.3. Encryption and Decryption

The same algorithm can be used for encryption or decryption.[4] The method described above will encrypt a block of plaintext and return a block of cipher text. In order to decrypt the cipher text and get the original plaintext again, the procedure is simply repeated but the sub keys are applied in reverse order, from K[16]-K[1]. That is, stage 2 of the

Core Function as outlined above changes from R[I-1] XOR K[I] to R[I-1] XOR K[17-I]. Other than that, decryption is performed exactly the same as encryption.

4. Programming Environment

As already described, we can use any programming environment. Now here we are using VLSI environment. So the hardware description language is used to build this design is Verilog HDL[12]. Different capabilities and features of Verilog lead to various implementation of the design in terms of performance and speed. Xilinx ISE 13.4 Design Suit is used as simulation tools and also for designing layout of synthesis. Similarly, other software and Hardware can be used and this algorithm can be easily implemented on them.

5. Implementation Results

a) Original image[9] b) Encrypted image c) Decrypted image

Figure 5. Thumb Impression

The First result is found on thumb impression in this a thumb impression is taken as trial as in fig. 5(a) and then it is converted into binary form, here it is a grayscale image so '0' will be give for a black and '1' will be given to white pixel.

Then the produced binary file is converted into hexadecimal for ease of feeding into simulator because 64 binary bits = 16 hex bits.

Then we get the encrypted hex file the it is again converted into binary to make the encrypted image as in fig. 5(b) then using DES decryption we get the decrypted image as in fig. 5(c) by decrypting the encrypted image by providing the same key used in the Encryption which is possible to provide by only authorized user, who knows about the key.

a) Original image[9] b) Encrypted image c) Decrypted image

Figure 6. Retinal scan[9]

The next application is on Iris scan which is same as in case of thumb impression of fig. 5 here fig. 6(a) is the original iris scan image and by DES of its hex file we get the encrypted iris image and using Decryption we get the decrypted image as shown in fig. 6(b) and (c) respectively.

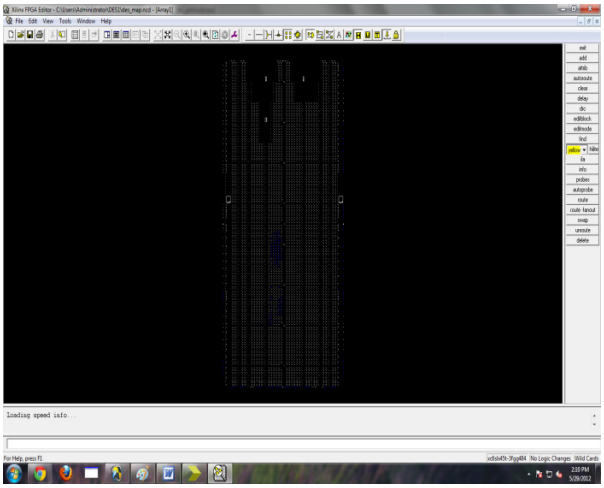

Figure 7. chip Graphics formation on Xilinx

Fig. 7 Shows the Chip Graphics Formed using Xilinx ISE 13.4 tools which can be used directly for manufacturing the Unique Chip.

5.1. Comparison with other Algorithms

Here we compare this DES algorithm with respect to ease of implementation and no. of bits used. Here the comparison is made with the most commonly used other algorithm such as triple- DES (Data Encryption Standards), Advanced Encryption Standards (AES) (Rijndael) and Blowfish.

Table 1. Algorithm comparison

Algorithm	Key Size (Bits)	Block Size (Bits)
DES	64	64
3DES	192	64
AES (Rijndael)	256	128
Blowfish	448	64

So it is clear from the above comparison that the DES is the better encryption algorithm as compare to others because it uses a fixed 64 bit key as well accepts a 64 bits block size so it increases the ease of implementation on verilog HDL in Xilinx ISE 13.4 tools.

So we can see that using DES for image encryption is a new kind of application in image security and it is a novel example of encryption algorithm in image encryption having ease of application and we can use its further application also in Video encryption that will be a new aspect.

6. Conclusions and Future Work

As we can use any Design platform however, by using Xilinx ISE 13.4 the complete Chip level solution can be used in Unique ID database encryption (of original Image data).We know each citizen has Unique ID & their Biometric Image is saved in a file with same ID name. Then Chip will encrypt all information just after formation of Unique ID (UID) & then only encrypted Image will store in memory Device & then it will send to Central Server of Country. The DES key in not known to any citizen, officials & also to

central server. So it becomes more secure. Same Key is used for encryption of all citizens' data, so multiple copies of same chip can be formed for use at different locations of country. Only authorized citizen can access his/her data ,After giving genuine input of his finger print or iris scan etc.After Decryption of stored data of given UID no. and comparison with input scan further access to that person will be allowed.

So this design can be applied as a future work in this area of national security.

ACKNOWLEDGEMENTS

I owe my profound gratitude to my supervisor Dr. R.S. Meena, for their valuable guidance, supervision, constant support and encouragement which have made me as a constant oasis of ideas and passion in science which exceptionally inspire and enrich my knowledge to pursue this Research work.

And a very big thanks you to my all respective teachers and beloved family and all my friends who have been a pillar of support during the arduous times of my research.

REFERENCES

[1] William Stallings, "Cryptography and network security', 3rd edition.

[2] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani, " A New Modified Version of Advance Encryption standard Based Algorithm for Image Encryption", ICEIE 2010 Volume-I, VI-141 to VI-145

[3] Arup Kumar Pal,G. P. Biswas,S. Mukhopadhyay, "Designing of High-Speed Image Cryptosystem Using VQ Generated Codebook and Index Table " , 2010 International Conference on Recent Trends in Information, Telecommunication and Computing Pp.:39-43

[4] K.Deergh Rao, Ch.Gangadhar,"VLSI Realization of a secure cryptosystem for Image Encryption and Decryption", 2011 IEEE Pp.:543-547

[5] National Bureau of Standard-Data Encryption Standard, FIPS Publication 46, 1977

[6] William Stallings, "Network Security Essentials (Application and Standards)", Pearson Education, 2004.

[7] Yong-Hong ZHANG,"Image Encryption Using Extended Chaotic Sequences" 2011 Fourth International Conference on Intelligent Computation Tech. & Automation, Pp.:143-146

[8] Ling Bin Liu Liden, Zhang Jan,"Image Encryption algorithm based on chaotic map and S-DES" 2010 IEEE Pp.:41-44

[9] http://en.wikipedia.org/wiki/File:Humaniris.jpg

[10] http://en.wikipedia.org/wiki/Fingerprint

[11] http://en.wikipedia.org/wiki/Data_Encryption_Standard

[12] Saeid Taherkhani, Enver evr, Orhan Gemikonakli," Implementation of Non-pipelined and Pipelined DES using Xilinx Virtex-6 FPGA Technology", 10th IEEE international Conference CIT 2010, Pp.:1257-1262