FPGA Based Implementation of Image Encryption Using Scan Patterns and Carrier Images

Yukthi.B.R, Savitha.A.P, M.B.Anandaraju, Nuthan.A.C

Abstract— This paper presents an FPGA implementation of image encryption method using carrier images and scan patterns generated by scan methodology. The scan is a language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths. Then scanning paths sequence fill in original image. The carrier image is created with the help of alphanumeric keyword. Each alphanumeric key will be having a unique 8bit value generated by 4 out of 8-code.This newly generated carrier image is added with the original image to obtain encrypted image. The scan methodology is applied to either original image or carrier image, after the addition of original image and carrier image to obtain the highly distorted encrypted image. By applying the reverse we get the decrypted image. Reversible logic is most popular concept in energy efficient computations and this will be demand for upcoming future computing technologies. The proposed paper will be simulated using Xilinx simulator and implemented in Xilinx FPGA platform.

Index Terms— Carrier image, Encryption, Scan patterns, 4 out of 8-code.

I. INTRODUCTION

With the ever increasing growth of multimedia applications, security is an important issue in communication and storage of images. Image encryption has applications in internet communication, multimedia system, medical imaging, telemedicine, and military communication.

Information is an asset that has a value like any other asset. As an asset, information needs to be secured from attacks. Because of the characteristic of digital images, some security problems come out besides the extensive usage of these images. The importance of securing information/image has reached its highest level in the recent year due to hacker attack and instruction of people's privacy.

Cryptography is popularly known as an art and science of secret writing. This enables us to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. S.R.M. Prasanna and Y.V. Subba Rao have presented the method which employs magnitude and phase manipulation using carrier images [1].

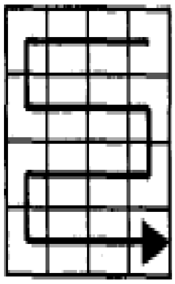
The novelty of this paper explains the concept of carrier images for encryption process. Chan-shen chen and Rong-jain chen proposed an image encryption and decryption algorithm based on scan methodology [2]. In [3] S.S. Maniccam and N.G. Bourbakis have presented a method for image and video encryption, here first stage lossy video compression based on frame difference before the encryption. Here they say image encryption is performed by scan-based permutation of pixels and substitution rule which together form an iterated product cipher. We implemented an encryption method which involves three steps; first step is constructing a size extended binary image using original image. In second step, applying the existing SCAN patterns to rearrange the pixels of extended binary image and finally in third reconstruct the gray scale image to obtain the encrypted version [4]. We also developed the concept of generating the carrier image with the help of unique code called as 4 out of 8-code, by adding the carrier image to original image we get the encrypted image [5].

II. IDEA BEHIND THE PROPOSED WORK

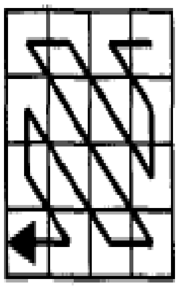
There are several method foe image encryption which deals in their own ideas. In few encryption algorithms, encryption process depends only on the keywords, but in some algorithms they use only carrier image for encryption. Anyhow, we have an idea to hybrid the existing algorithms to get a new path for encryption by taking the advantages of individual methods. Hence come up with the concept of hybridizing the carrier image and scan pattern for image encryption to get the highly distorted image.

III. OVERVIEW OF SCAN PATTERNS

A scanning of two dimensional arrays is an order in which each element of the array is accessed exactly once. Scan is a formal language-based two-dimensional spatial-accessing methodology which can represent and generate a large number of wide varieties of scanning paths. Scan language uses four basic scan patterns. They are continuous raster C, continuous diagonal D, continuous orthogonal O and spiral S. Each basic pattern has 8eight transformation numbered from 0 to 7. For each basic scan pattern, the transformations 1, 3, 5, 7 are reverses of transformation 0, 2, 4, 6 respectively. The basic scan patterns are shown in the Figure 1.



(a) Continuous raster C



(b) Continuous diagonal D

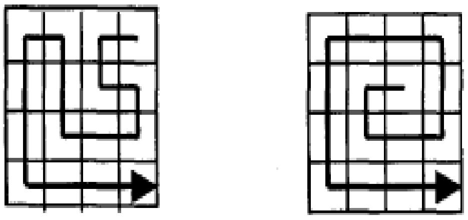
Manuscript received June, 2013.

Yukthi.B.R, PG Student, VLSI Design and Embedded System, B.G.S. Institute of Technology, B.G.Nagar, Mandya-571448, Karnataka, India.

Savitha.A.P, Associate Professor, Department of Electronics and Communication Engineering, B.G.S. Institute of Technology, B.G.Nagar, Mandya-571448, Karnataka, India.

Prof. M.B.Anandaraju, Professor and HOD, Department of Electronics and Communication Engineering, B.G.S. Institute of Technology, B.G.Nagar, Mandya-571448, Karnataka, India.

Nuthan.A.C, Assistant Professor, Department of Electronics and Communication Engineering, G. Madegowda Institute of Technology, Bharathinagara, Mandya-571422, Karnataka, India.



(c) Orthogonal O (d) Spiral S

Figure 1 Basic Scan Patterns

IV. CARRIER IMAGE CREATION

Here a new code called 4 out of 8-code is defined. This code is of 8 bit length with 4 numbers of one's and 4 number of zero's and we made one consideration that each nibble must have two numbers of ones and two number of zeros. We listed all 36 possible combination of the 4 out of 8-code and each code is assigned to an alphanumeric character in table 1. Since 26 alphabets (capital letters or small letters) and 10 numerals forms to give 36 alphanumeric characters, this code is more suitable to assign a unique code to each alphanumeric character.

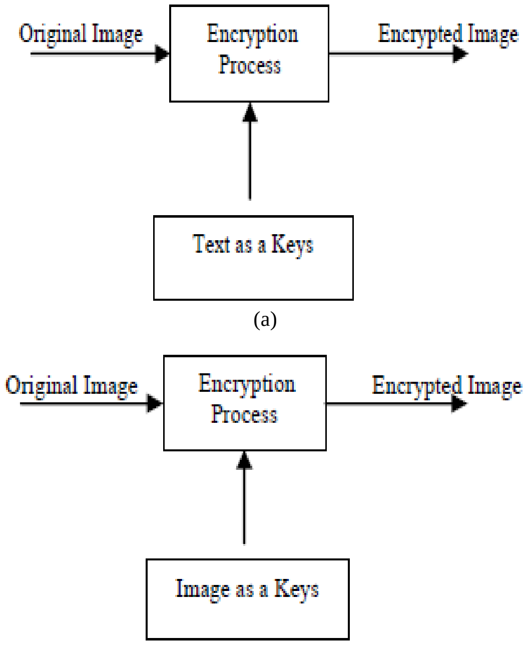
As we enter the different the different keyword, each keyword is taken and rearranged in matrix form of equal size of the original image. If the length of the keyword is very small then the same keyword is repeated till length becomes equal to the size of the original image. By using the look up table of the alphanumeric character and 4 out of 8-code shown in TABLE 1, a carrier image is created. Depending upon the keyword, carrier image is created and used in the addition process to generate an encrypted image.

TABLE 1
36 POSSIBLE COMBINATION OF 4 OUT OF 8 CODE

SL NO.	BIN	HEX	DEC	ALPHA NUMERIC
1	00110011	33	51	A,a
2	00110101	35	53	B,b
3	00110110	36	54	C,c
4	00111001	39	57	D,d
5	00111010	3A	58	E,e
6	00111100	3C	60	F,f
7	01010011	53	83	G,g
8	01010101	55	85	H,h
9	01010110	56	86	I,i
10	01011001	59	89	J,j
11	01011010	5A	90	K,k
12	01011100	5C	92	L,L
13	01100011	63	99	M,m
14	01100101	65	101	N,n
15	01100110	66	102	O,o
16	01101001	69	105	P,p
17	01101010	6A	106	Q,q
18	01101100	6C	108	R,r
19	10010011	93	147	S,S
20	10010101	95	149	T,t
21	10010110	96	150	U,u
22	10011001	99	153	V,v
23	10011010	9A	154	W,w
24	10011100	9C	156	X,x
25	10100011	A3	163	Y,y
26	10100101	A5	165	Z,z
27	10100110	A6	166	0
28	10101001	A9	169	1
29	10101010	AA	170	2
30	10101100	AC	172	3
31	11000011	C3	195	4
32	11000101	C5	197	5
33	11000110	C6	198	6
34	11001001	C9	201	7
35	11001010	CA	202	8
36	11001100	CC	204	9

V. PROPOSED WORK

Image encryption can be done at different stage or in multiple stages in multiple ways. If the encryption process is only in single stage then security is less compared to multistage encryption. Figure 2 shows the block diagram of existing encryption approach using text as a keyword and image as a keyword.



(a)

(b)

Figure 2 Block Diagram of Existing Image encryption Approach Using (a) Text as a Key (b) Image as a key

Encryption process may take different approaches, for example encryption may be using SCAN method or only by phase-magnitude manipulation method or using only carrier image generated by 4 out of 8 code. Figure 3 shows the block diagram of proposed hybrid approach which contain multiple keywords, where key-1 is corresponding to create a carrier image and key-2, key-3, key-4, along with SCAN encryption process are optional.

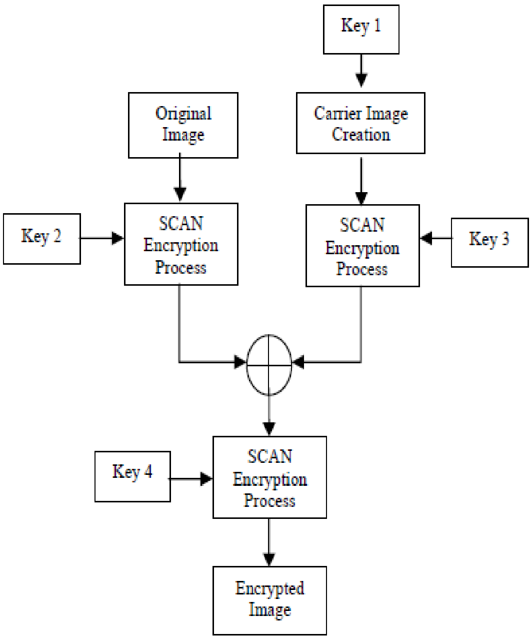


Figure 3 Block Diagram of Proposed Image Encryption Approach Using SCAN Patterns and Carrier Images

VI. RESULTS

The entire architecture is modeled using VHDL. The coding is done on Xilinx ISE12.2 on Spartan 3. Figure 4, Figure 5, Figure 6 and Figure 7 shows the simulation result of encrypted data using SCAN patterns.

Figure 4 shows the simulation result of encrypted data using spiral scan. Figure 5 shows the simulation result of encrypted data using orthogonal scan. Figure 6 shows the simulation result of encrypted data using diagonal scan and Figure 7 shows the simulation result of encrypted data using continuous scan. Fgure 8 shows the simulation result of carrier image. Figure 9 shows the encrypted data using scan methodology. Figure 10 shows the total encrypted data using carrier image and scan patterns.

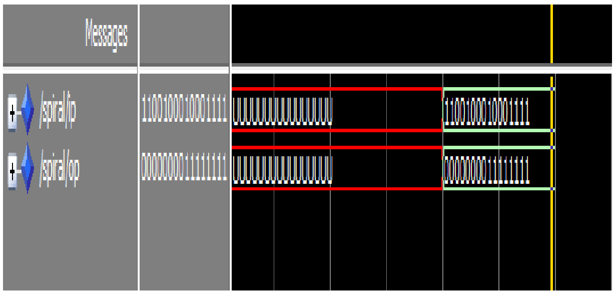


Figure 4 Simulation result of Encrypted Data Using Spiral Scan

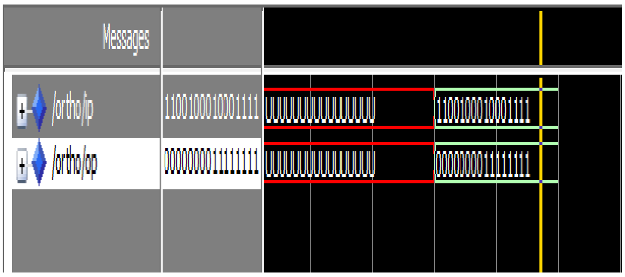


Figure 5 Simulation result of Encrypted Data Using Orthogonal Scan

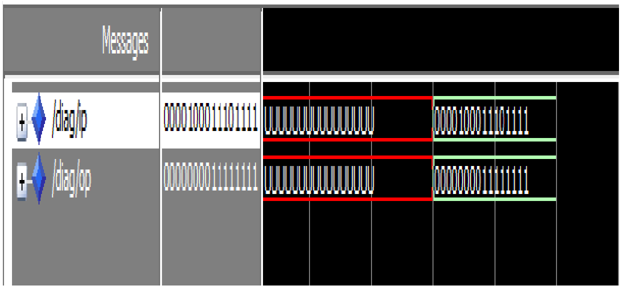


Figure 6 Simulation result of Encrypted Data Using Diagonal Scan

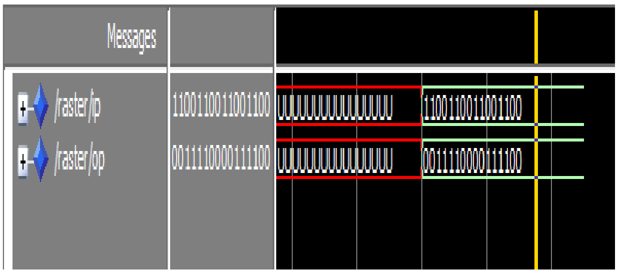


Figure 7 Simulation result of Encrypted Data Using Continuous Raster Scan

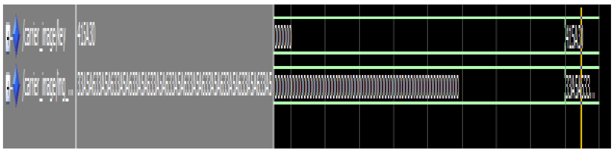


Figure 8 Simulation result of Carrier image

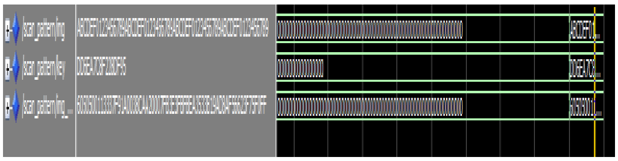


Figure 9 Simulation result of Scan Encrypted Data

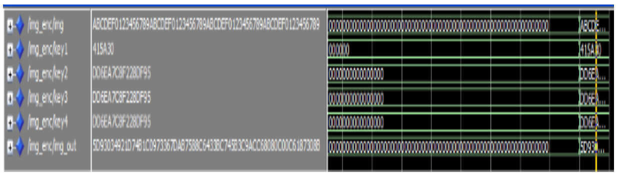


Figure 10 Simulation result of Total Encrypted Data

VII. APPLICATIONS

Image encryption has many applications. Some important areas include the following [2]

- Internet Communication.
- Multimedia Systems.
- Medical Imaging.
- Telemedicine.
- Military Communication.

VIII. CONCLUSION AND FUTURE WORK

This paper presents an efficient approach for implementation of Image Encryption. The existing approach is done in Matlab, but here we have done the proposed approach in FPGA. For the sake of simplicity we used only few SCAN patterns and few carrier keywords, but proposed algorithm also works for complex SCAN patterns and complex carrier keywords. As the complexity increases the encrypted image is more distorted as compare to the result of single stage encryption. In future we want to develop hybrid algorithm which uses more SCAN patterns, carrier images along with some bit manipulation technique to provide more security to the images.

REFERENCES

[1] S.R.M Prasanna, Y.V. Subba Rao and A. Mitra., “An Image Encryption method with Magnitude and Phase Manipulation using carrier images”, *IJCS*, vol. 1,No 2, pp.132-137,2006.

[2] Chao Shen Chen and Rong Jian Chen “Image encryption and decryption using SCAN methodology,” *Proc. PDCAT*, 2006.

[3] S.S. Maniccam and N.G.Bourbakis, “Image and video encryption using SCAN patterns,” *Pattern Recognition, vol*.37, pp.725-737, 2004.

[4] Panduranga H.T, Naveenkumar s.k, “A novel 3-step combinational approach for image encryption”, *IJCEIT, vol* 03, 2009.

[5] Panduranga H.T, Naveenkumar s.k, “A novel image encryption method using 4outof8 code”, *Proc. CommV’09*, pp 460-462, 2009.

Yukthi.B.R pursuing 4th semester M.Tech VLSI Design and Embedded System in B.G.S. Institute of Technology, B.G.Nagar, Mandya, Karnataka, India. She completed her B.E. from Government Engineering College Hassan, Karnataka in 2011. Her area of interest includes Embedded system, Low power VLSI, Cryptography and System on-chip.