Research Paper

Engineering

VHDL IMPLEMENTATION OF SCRAMBLING FOLLOWED BY ENCRYPTION FOR PROVISION OF CONFIDENTIALITY TO DIGITAL IMAGES

S Skandha Deepsita

Department of Electronics and Communication Engineering,
Narayana Engineering College, Nellore, Andhra Pradesh, India

ABSTRACT

Transmission of secured data is vital in the fields of internet communications, telemedicine, military communications etc and information security is one of the important issues to be addressed. It is very much essential to excogitate the ways to resolve. The security issues can be one or more than one of CIA trio. This paper focuses on providing confidentiality to the digital images. The proposed approach is, scrambling the image followed by encryption. The combination of two algorithms provides better Security Quality Factor and also low correlation coefficient. This is implemented by using hardware description language because HDL accelerates the design of algorithms for image processing on hardware. Implementation is done in VHDL using XILINX ISE design suite.

KEYWORDS : Digital images, Confidentiality, VHDL, XILINX ISE.

1. INTRODUCTION

With the advancement of technology, the cyber crime rate is also growing up. So there is a great demand for providing security to information during transmission. Images being the highest percentage among the digital media, the provision of security to images is vital. The security problems can be divided roughly into four areas, namely, secrecy, authentication, non-repudiation and integrity control. Confidentiality which is one of the facets of CIA trio is protecting the information from disclosure to unauthorized parties.

Scrambling can be done either in spatial or frequency domain. It modifies the actual information in such a way that original semantics are lost and transformed into completely new image. The restoration can be done only by user who knows the algorithm and key [1].

Cryptography is the field of study of encryption and decryption. The art of breaking ciphers, known as cryptanalysis, and the art of devising them are collectively known as cryptology. In particular the cryptographic algorithms can be either symmetric or asymmetric. A cipher is a character-for-character or bit-for-bit transformation.RC5 is symmetric block Cipher which was first designed by Ron Rivest. Block ciphers are used for bulk encryption of long streams of data [2-4].

Rather than implementing the scrambling and cryptography to data independently, combined application of these algorithms provides better confidentiality.

2. LITERATURE SURVEY

Variety of scrambling algorithm for images has been proposed in the literature. Some of the algorithms are Hilbert space filling curve, Caesar/affine, Gray code transformation and DES based scrambling [5,6]. Diverse cryptographic algorithms have been proposed in the literature. Symmetric key algorithms are RC2, AES, 3DES, SEED, XTEA. Asymmetric key algorithms are RSA, DSA, YAK, etc [7]. Combining the digital image scrambling with one of the cryptographic algorithms is proposed by previous researchers. Image scrambling based on Chaos theory and Vigenere. This has key length of 'N' which is total number of pixels in the image. The key space is N! and hence images are more prone to brute force attacks. Scrambling based on parameter based on 'M' sequences [8].

3. METHODOLOGY

The design process contains five modules as given in the following diagram.

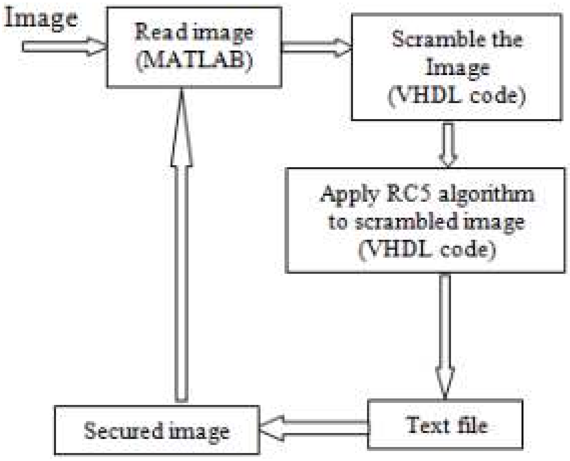
Image
Read image (MATLAB)
Scramble the Image (VHDL code)
Apply RC5 algorithm to scrambled image (VHDL code)
Text file
Secured image

Figure 1: Block diagram of proposed algorithm

3.1. Evaluation Tools

The two evaluation tools used in this work are correlation coefficient and security quality factor.

3.1.1. Correlation coefficient

Correlation coefficient is the ratio of covariance to the square root of product of independent variances of two random variables. Here the original input image is one random variable and scrambled/encrypted image is another random variable.

$$\sigma = \frac{co\ (A,B)}{\sqrt{va(A) * va(B)}} \qquad (1)$$

Where σ is correlation coefficient for A and B, co is covariance and va is variance.
co (A,B) = [E(A-E(A))(B-E(B))],

Where E is expectation.
Where A is original image and B is scrambled/encrypted image.
It is a statistical measurement of similarity between two variables. Its value can be 0 or 1, which means entirely different or same respectively. Zero value indicates better security.

3.1.2. Security Quality Factor (S)

It is average difference between the input image histogram and scrambled/encrypted image histogram. Histogram is the intensity distribution of gray level image and is said to be in the range of [0, L-1], where L is intensity level.

Where M is the size of image and I(i) is the original image histogram and I(i1) is the scrambled/encrypted image histogram. The M value considered here is 256. High value of S is required.

3.1. Design phases

There are three design phased followed by security evaluations. They are scrambling, applying RC5 algorithm, combination of both algorithms [9-11]

3.1.1. Scrambling of digital image

Scrambling algorithm does the coding operation which randomizes the data. The input to the scrambling algorithm is the plain image and the scrambled image is denoted by S. data is scrambled using n-bit serial-in parallel-out shift register.

Figure 2: Block diagram of proposed algorithm

$S=E+S*(a_1B^1+a_2B^2+a_3B^3+\ldots+a_NB^{N)})^N$(3)

$S = E+Y*B$ (4)

$Y = S* (a_1+a_2+a_3+\ldots\ldots+a_N)$ (5)

$S = E+K$, where $K=YB$

D^nB gives the sequence B delay by N units.
Here + denotes modulo-2 addition and the value of a_j can be 0 or 1.
$a_i=0$ => no connection is taken from the j^{th} stage.
$a_i=1$ => connection is taken from the j^{th} stage.

Thus Y depends on gain values and number of stages of shift registers. The complexity of Y increases with N and hence hides the actual information from unauthorized accesses.

3.1.1. Implementation of RC5 algorithm

Rc5 is a 32 or 64 bit cipher designed for security of RSA. It has variable number of rounds and size of words and it comes under the class of symmetric block cipher and this algorithm is suited for both hardware and software. This is said to have high security because the rotation is dependent on data.
1. Implement RC5 cipher
2. Get the 512 bit key
3. Change the digital image into blocks
4. Encrypt the image using the generated RC5 key.

3.2.3. Combination of both algorithms

The output of phase I i.e., scrambled image is fed as input image for phase II i.e., encryption. The security evaluations are done for the three phases. The proposed algorithm is coded in VHDL using XILINX ISE.

4. RESULTS AND DISCUSSIONS

The proposed scheme is simulated for functional verification using XILINX ISE and the output images are observed in MATLAB. The original input image is shown in the Figure 3(a). The results are shown in the Figure 3 (b, c).

Figure 3: (a) Input image; (b) Scrambled image; (c) Output image.

Table 1: Comparison of individual algorithms

Table 2: Combination of both algorithms

Correlation coefficient for scrambling is found to be almost zero; however, the intensity distribution remains same leading to low value of S. In contrast RC5 algorithm has high value of S but also high correlation coefficient which is shown in the Table 1. Combining both algorithms results in high value of S and low value of σ and hence providing high confidentiality to images. Table 2 shows that the results of proposed work for two different images.

The hardware obtained by coding algorithms in VHDL is as shown in the Figure 4 and Figure 5. The synthesis reports are developed using XILINX ISE designs suite and is shown in the Figure 6 (a & b).

Figure 4: RC5 algorithm VHDL hardware

Figure 5: Scrambling VHDL hardware