iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4154

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Highly Randomized Digital Watermarking for Image and Video Applications

P. Dharsana[1], G. Latha[2]
Assistant Professor, Department of Electronics and Communication Engineering,
Apollo Engineering College, Chennai, Tamil Nadu, India

Abstract: ***Watermarking as an additional tool in protecting digital content. The robustness of transformed domain watermarking concept with Cryptography including the various schemes of system based on the kind of key and a few algorithms such as DCT and RC5. The detail mathematical foundations for RC5 based systems, and possibilties of DCT macro block conversion and its physical domain transformation properties. And finally the computational and security metrics of DCT is proved and their complexity reduction were also analysis using FPGA hardware synthesis. Finally, considering the power consumption as one of the critical factors in FPGA or ASIC designs, the mentioned image FSM enabled DCT transformed encryption schemes can be design and optimize for low power implementations.***
Keywords: Wavelet transform, Discrete Cosine Transform, Lfsr, Watermarking, Stegnography.

I. INTRODUCTION

Data hiding, watermarking, and Steganography are perhaps, a curious association of words. And not only in English, because equally odd related terms are in use in other languages: just for instance, Spanish, French or Italian have used, for similar purposes, digital filigreeing, invisible stamping, numerical tattooing, electronic marking, and others. But these expression do not refer at all to craftsmanship, postal services, or body art, let alone some more or less hermetical or occultist skills. Rather, this richness of terms mirrors the flurry of activity that has surrounded in recent times the main subject investigated in this thesis.

An increasing amount of information is transmitted over the Internet, including text and audio, image, and other multimedia files. Images are widely used in daily life, and, as a result, the security of image data is an important requirement. In addition, when communication bandwidth or storage is limited, data are compressed. In particular, when a wireless communication network is used, low-bit-rate compression algorithms are needed as a result of bandwidth limitations. Encryption is also performed when it is necessary to protect user privacy . non chaos-based methods. Image encryption can also be divided into full encryption and partial encryption (also called selective encryption) schemes according to the percentage of the data that is encrypted. Encryption schemes can also be classified as either combined-compression methods or non-compression methods.

But, as computers and Internet connections have pervaded the developed world along with the globalization tide, the digital overturn has also been a silent Trojan horse that has afforded millions of people to get, duplicate, manipulate, and/or distribute original digital data. The shock that this upheaval has caused to the traditional information flow model is far from being over, and it promises to keep attracting the attention of both researchers and society for many years to come. To start with, the standard framework used to control revenues and property the cornerstones of market-oriented economies has been shaken at its foundations.

Although legal provisions in force would seem to remain roughly applicable in the Digital Age, new technical tools are needed for law enforcement inside a world in which information moves and changes at a vertiginous speed . As a result, new shades have appeared over seemingly plain old concepts. One of the most outstanding among them is that of copy, one of the ever favorite pastimes of mankind. Copy has always been an unrelenting instrument of progress, there included copy in the sense beloved by Borges imperfect copy as sometimes a happy mutation is preferable to a sterile perfect duplication.

II. BACKGROUND

A. Wavelet Transform

The transform of a signal is a form of representing the signal. It does not change the information present in the signal. The Wavelet Transform provides a frequency representation of the signal. It is developed to avoid the short coming of the Short Time Fourier Transform (STFT), which be used to analyse non-stationary signals. The Wavelet Transform uses multi-resolution technique by which frequencies are checked with various resolutions.

A wave is an oscillating function of time and is periodic. In contrast, wavelets are localized waves. It has energy concentrated in

time and are used to analyse the transient signals. While Fourier Transform and STFT make use of waves to analyze signals, the Wavelet Transform uses wavelets of finite energy.

B. The Discrete Wavelet Transform and the Wavelet Series

The Discrete Wavelet Transform (DWT) is provided by equation 1.1, where x(t) is the signal to be analyzed. ψ(t) is the mother wavelet. All the wavelet functions used here are derived from the mother wavelet through shifting and scaling.

$$X_{WT}(\tau, s) = \frac{1}{\sqrt{|s|}} \int x(t) \cdot \psi^* \left(\frac{t-\tau}{s} \right) dt$$

The mother wavelet is used to produce all the basic functions are designed based on some characteristics associated with that function. The parameter τ is related to the location of the wavelet function as it is shifted through the signal. Thus, it corresponds to the information in the Wavelet Transform. The scale parameter s is defined as 1/frequency and corresponds to frequency information.

III. LITERATURE SURVEY

Steganography is the art of hiding information by embedding messages within other, seemingly harmless messages. Steganography means "covered writing" in Greek. As the goal of steganography is to hide the presence of a message and to create a covert channel, it can be seen as the complement of cryptography, whose goal is to hide the content of a message.

The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present." By using this proposed algorithm, we can hide our file of any format in an image and audio file. We can then send the image via e-mail attachment or post it on the web site and anyone with knowledge that it contains secret information, and who is in possession of the encryption password, will be able to open the file, extract the secret information and decrypt it.

Steganography literally means covered writing. Its goal is to hide the fact that communication is taking place. In the field of Stenography, some terminology has been developed. The term cover is used to describe the original message, data, audio, still, video and so on. The growing possibilities of modem communications need the special means of security especially on computer network. The network security is becoming important as the number of data being exchanged increases.

Therefore, the confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an explosive growth in the field of information hiding. In addition, the rapid growth of publishing and broadcasting technology also requires an alternative solution in hiding information. The copyright of digital media such as audio, video and other media available in digital form may lead to unauthorized copying. This is because the digital formats make it possible to provide high image quality under multi-copying.

Unauthorized copying is of great problem of especially to the music, film, book and software publishing industries. To overcome this problem, some invisible information can be embedded in the digital media in such a way that it could not be easily extracted without a specialized technique. Information hiding is an emerging research area, which includes applications such as copyright protection for digital media, watermarking, fingerprinting, and Stenography. All these applications of information hiding are quite diverse.

IV. PROPOSED SYSTEM

A. Image Processing System

Multimedia data processing encompass every aspects of our daily life such as communication broad casting, advertisement, video games, etc has become an integral part of our life style. The most significant part of multimedia systems is application involving image or video, which require computationally intensive data processing.

Multimedia files are large and needs lots of hard disk space. The files size makes it time-consuming to move them from place to place over school networks or to distribute over the Internet. Compression shrinks files, making them smaller and more practical to store. Compression works by removing repetitious or redundant information, effectively summarizing the contents of a file in a way that preserves as much of the original meaning as possible.

In order to reduce the volume of multimedia data, compression techniques are widely used. Efficiency of a transformation scheme can be directly gauged by its ability to pack input data into as few coefficients as possible. This allows the quantizer to discard

coefficients with small amplitudes.

B. Discrete Cosine Transform

Discrete cosine transform (DCT) is a major compression schemes and has energy compaction efficiency greater than other transforms. The principle advantage of image transformation is the removal of redundancy between neighbouring pixels. This leads to uncorrelated coefficients which can be encoded independently. DCT has that de correlation property.

The transformation algorithm needs to be of low complexity. Since the DCT is separable 2-D can be obtained from two 1-D DCTs. The 2-D DCT equation is given by Equation (1)

$$C(u,v)=\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right], \quad (1)$$

For $u,v= 0,1,2,\ldots,N-1$.

The inverse transform is defined by Equation (2)

$$f(x,y)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right], \quad (2)$$

For $x,y= 0,1,2,\ldots,N-1$. The 2-D basis functions can be generated by multiplying the horizontally oriented 1-D basis functions with vertically oriented set of the same functions.

In image compression, the data is divided into 8x8 blocks of pixels. (From this point on, each colour component is processed independently, so a "pixel" means a single value, even in a color image.) A DCT is applied to each 8x8 block. DCT converts the spatial representation of image into a frequency map: the "DC" term represents the average value in the block, while successive higher-order ("AC") terms represent the strength of rapid changes across the width or height of the block. The highest AC term represents the strength of a cosine wave alternating from maximum to minimum at adjacent pixels.

C. Human Visual System (HVS)

In order to produce good watermarking algorithms, characteristics of the human visual system is studied. The nuances of visual perception has given scientists an insight into modelling watermarks that do not interfere with the host image. The still image to be compressed is passed through a coder, which transforms the image by ripping it into distinct blocks of 8*8 pixels. A DCT is applied on thus obtained distinct blocks.

1) DCT Algorithm: A semi-fragile watermark in DCT is developed here.

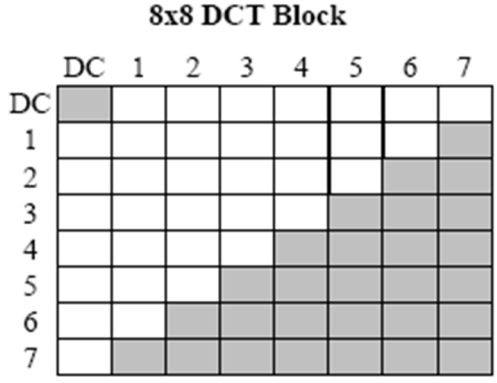


Fig3.1 8x8 DCT Block

Watermark is embedded in every 8*8 DCT block. Though each block has a different watermark, the watermark is embedded on the same indices of each block.

D. RGB to Lab Conversion

The proposed approach performs clustering of colour space. A particle consists of K cluster centroids representing L*a*b* colour triplets. The basic aim is to segment colours in an automated fashion using the L*a*b* colour space and K-means clustering. The entire process can be summarized in following steps :

Step 1: Read the image. Read the image from mother source which is in .JPEG format, which is a fused image.

Step 2: For colour separation of an image, apply the De-correlation stretching.

Step 3: Convert Image from RGB Color Space to L*a*b* Colour Space. How many colours we see in the image if we ignore variations in brightness? There are three colours: white, blue, and pink. It can be visually distinguish these colours from one another. The L*a*b* colour space (also known as CIELAB or CIE L*a*b*) enables us to quantify these visual differences. The L*a*b* colour space is derived from CIE XYZ tristimulus values.

Step 4: Label Every Pixel in the Image using the results from DCT value. For every object in our input, DCT returns an index corresponding to a pixel macro block. Encrypt each block using predefined key values.

Step 5: Create Images that Segment the Image by Color and intensity. Using visibility levels, we have to select objects in image.

E. Basic Primitives

RC5 has a variable word size, a number of rounds and a variable length secret key. RC5 is exactly designated as RC5-w/r/b, where w denotes word size in bits, the standard value is 16,32and 64 bits; r denotes number of rounds and allowable value ranges from 0 to 255; b denotes length of user's secret keyin bytes and the allowable value ranges from 0 to 255. The parameters we have used are RC5-32/12/16. RC5 consists of components such as Key expansion, Encryption and Decryption .

F. Key Expansion

This routine expands the user's secret key K to fill the expanded key array S, S resembles an array of t=2(r+1) random binary words determined by K. It uses two word-sized binary constants Pw and Qw.

G. Algorithm

A typical stream cipher encrypts plain text one byte at a time. A stream cipher is designed to operate one bit at a time or one units larger than a byte at a time. It is a representative diagram of stream cipher structure. In this structure a key is given as input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are appearing random. A pseudo random stream is the one that is generated by an algorithm but is unpredictable without the knowledge of input key. The output of the generator is called a key stream which combines one byte at a time with the plaintext stream using the bitwise exclusive-OR (XOR) operation. For example, if the next byte generated by the generator is 01101100 and the next plain text byte generated is 11001100, then the resulting byte is cipher text .

H. Key Scheduling Algorithm

To begin, the entries of S are set equal to the values from 0 through 255 in ascending order; that is;

S[0] = 0, S[1] = 1, ..., S[255] = 255. A temporary vector T is also created. If the length of the key K is 256 bytes, then K is transferred to T. Otherwise, for a key of length eleven bytes, the first eleven elements of T are copied from K and then K is repeated as many times as necessary to fill out T. These preliminary operations can be summarized as follows:

```
/* Initialization*/
for i = 0 to 255
do
S[i] = i;
T[i] = K[i Mod keylen];
```

Next we use T to produce the initial permutation of S. This involves starting with S[0] and going through to S[255], and, for each S[i], swapping S[i] with another byte in S according to a scheme dictated by T[i]:

```
/* Initial Permutation of S */
j = 0;
for i = 0 to 255
do
```

j = (j + S[i] + T[i])
mod
256;
Swap (S[i], S[j]);
Because the only operation on S is a swap, the only effect is a permutation.

I. Stream Generation

The input key is no longer used once the S vector is initialized. Stream generation involves starting with S[0] and going through to S[255], and, for each S[i], swapping S[i] with another byte in S according to a scheme dictated by the current configuration of S. After S[255] is reached, the process continues, starting over again at S[0]:

/* Stream Generation*/
i, j = 0;
while(true)
i = (i + 1)
mod256;
j = (j + S[i]) mod256;
Swap(S[i], S[j]);
t = (S[i] + S[j])
mod 256;
k = S[t];

To encrypt, XOR the value k with the next byte of plaintext. To decrypt, XOR the value k with the next byte of cipher text.

J. LSB Substitution

LSB Coding Least significant bit (LSB) coding is the simplest way to embed information in a digital pixel file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. In some implementations of LSB coding, the least significant bit of a sample is replaced with a message bit. One should consider the signal content before deciding on the LSB operation to use. For example, a sound file that is recorded in a bustling subway station would mask low-bit encoding noise.

To extract a secret message from an LSB encoded image file, the receiver accesses to the sequence of sample indices used in the embedding process. Instantaneously , the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform.

LSB coding has been completely embedded, leaving the remaining samples unchanged. For providing more security, however in that the first part of the image file will have different statistical properties than the second part of the image file that was not modified. Another way to embed is to pad the secret message with random bits for that the length of the message is equal to the total number of samples. Now the embedding process ends up changing far more samples than the transmission of the secret required. This increases the probability that would be attacker will suspect secret communication.

K. Secured Watermarking

In other words, Alice has to be cooperative in order to gain the compression ratios. More specifically, after getting each prediction error $e_{i,j}$ via (1), Alice applies the following uniform scalar quantization on $e_{i,j}$ with a parameter τ

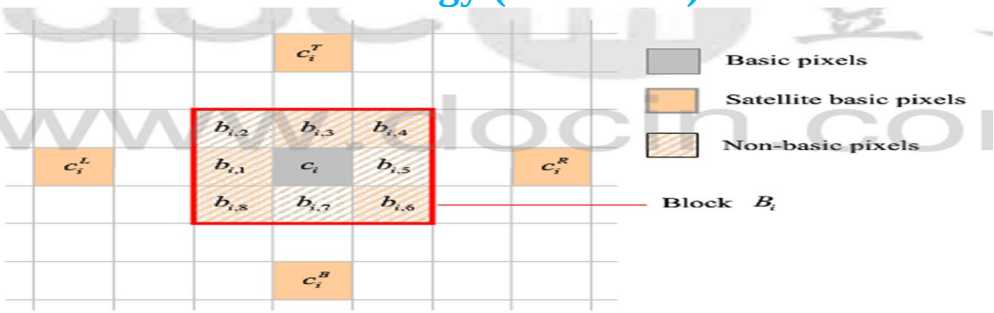
$$\check{e}_{i,j} = \lfloor (2\tau + 1)\lfloor (e_{i,j} + \tau)/(2\tau + 1) \rfloor \rfloor \text{ if } e_{i,j} \geq 0$$
$$\lfloor (2\tau + 1)\lfloor (e_{i,j} - \tau)/(2\tau + 1) \rfloor \rfloor \text{ if } e_{i,j} < 0 \quad (10)$$

where $\check{e}_{i,j}$ denotes the quantized version of $e_{i,j}$. Meanwhile, Alice maintains a reconstruction

$$\hat{I}_{i,j} = \tilde{I}_{i,j} + \check{e}_{i,j} \quad (11)$$

which will be used to predict the subsequent pixels and establish the context models.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



Prediction values p1,1 = 1/3 (2ci +ci L)
Prediction values p1,2 = 1/3 (ci +ci L + ci T)
Prediction values p1,3 = 1/3 (2ci +ci T)
Prediction values p1,4 = 1/3 (ci +ci T +ciR)
Prediction values p1,5 = 1/3 (2ci +ci R)
Prediction values p1,6 = 1/3 (ci +ci R + ci B)
Prediction values p1,7 = 1/3 (2ci +ci B)
Prediction values p1,8 = 1/3 (ci +ci B + ci L)
Prediction errors =bi,j - pi,j
Let w be bit to be embedded
Modified prediction eror will be,,
From the histogram of prediction error we can find P+, P-, Z+,Z-

$$e'_{i,j} = \begin{cases} e_{i,j} & \text{if } w = 0, \\ e_{i,j} + 1 & \text{if } w = 1 \text{ and } e_{i,j} = P_+, \\ e_{i,j} - 1 & \text{if } w = 1 \text{ and } e_{i,j} = P_-. \end{cases}$$

(b) Otherwise, no bit can be embedded and $e_{i,j}$ has to be modified to $e'_{i,j}$

using the rules:

$$e'_{i,j} = \begin{cases} e_{i,j} + 1 & \text{if } P_+ < e_{i,j} < Z_+, \\ e_{i,j} - 1 & \text{if } Z_- < e_{i,j} < P_-, \\ e_{i,j} & \text{otherwise.} \end{cases}$$

L. Permutation Performance

Only small amount of inter-dependence exists in the prediction error sequence. Compared with the traditional predictive coding system in which the compression is conducted over the original, unpermuted prediction error sequences, the compression task of Charlie has to be performed over the *permuted* ones. From the perspective of information theory, a sequence with inter-dependence, which is caused by redundancy, is more compressible than its i.i.d counterpart. As the permutation operations in the prediction error domain destroy the inter-dependence, the resulting ˜**C***k* is less compressible than its original, unpermuted version **C***k* . Fortunately, the inter-dependence left in each **C***k* is rather limited, thanks to the superior de-correlation capability of image predictors. Hence, it is intuitively expected and will be verified by our experiments that the coding penalty caused by prediction error permutation is very small.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V. RESULTS AND DISCUSSIONS

A. Matlab Output

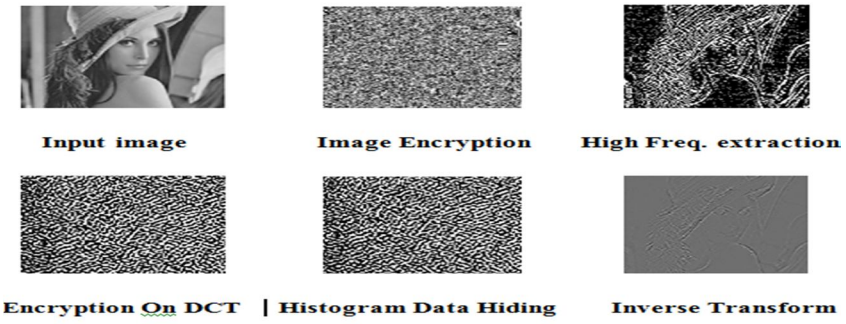


Fig .A GUI Image Encryption

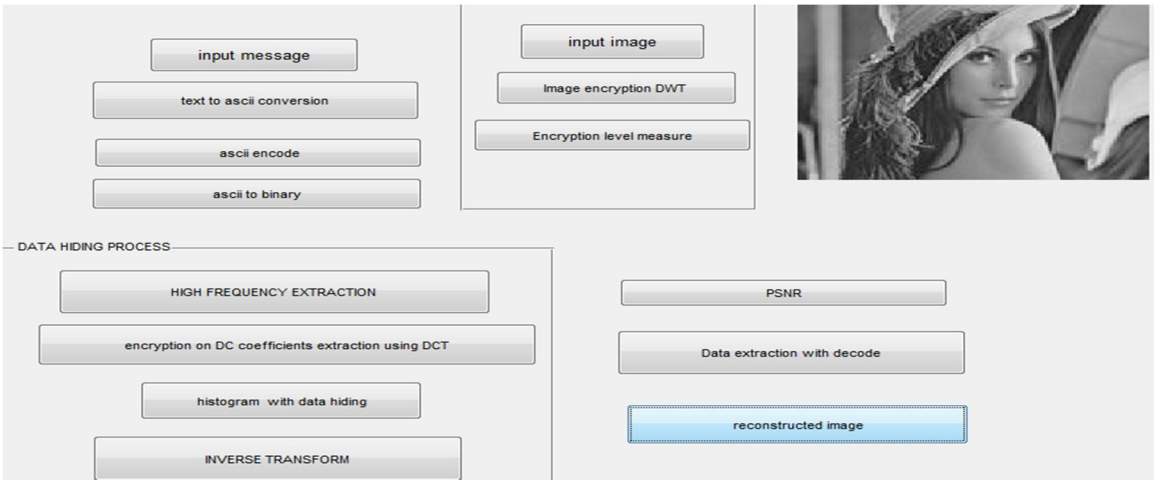


Fig. Reconstructed Image

1) *Description:* The above figure shows the reconstructed watermark image. The PSNR reading should be taken along with the measure of encryption level.

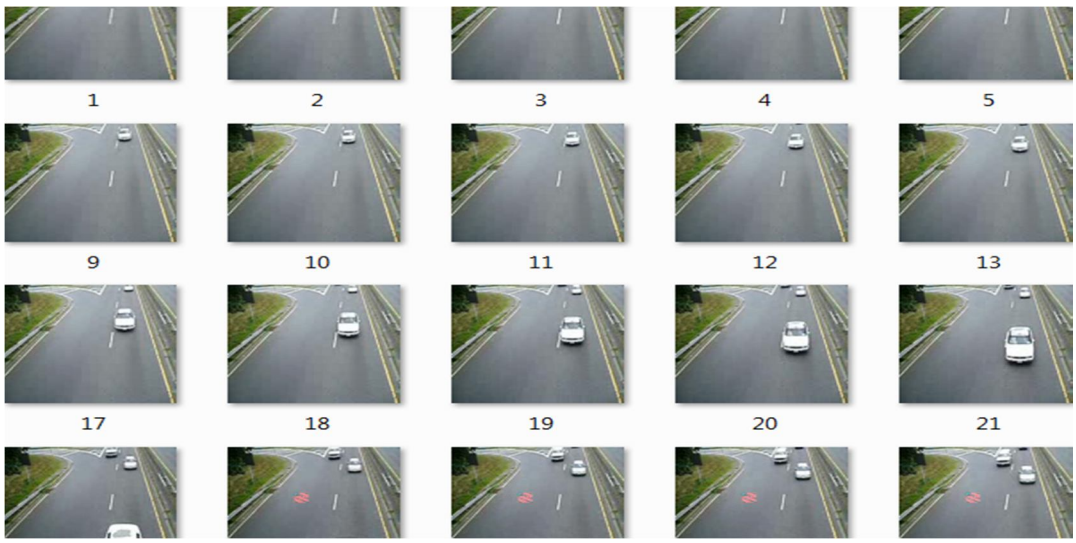


Fig. Frame Output

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. Area Utilization Report

Flow Summary

Flow Status	Successful - Sun Apr 02 16:33:33 2017
Quartus II Version	9.0 Build 132 02/25/2009 SJ Web Edition
Revision Name	UU
Top-level Entity Name	CODEC_MODULE
Family	Cyclone III
Met timing requirements	N/A
Total logic elements	12,006 / 24,624 (49 %)
Total combinational functions	11,295 / 24,624 (46 %)
Dedicated logic registers	4,277 / 24,624 (17 %)
Total registers	4277
Total pins	134 / 216 (62 %)
Total virtual pins	0
Total memory bits	0 / 608,256 (0 %)
Embedded Multiplier 9-bit elements	4 / 132 (3 %)

Fig 5.2. Flow summary report

C. Performance Report

Fmax Summary

	Fmax	Restricted Fmax	Clock Name	Note
1	56.1 MHz	56.1 MHz	clk	

Fig. Fmax summary report of slow corner

Fmax Summary

	Fmax	Restricted Fmax	Clock Name	Note
1	99.61 MHz	99.61 MHz	clk	

Fig. Fmax summary report of fast corner

D. Power Analysis

Flow Summary

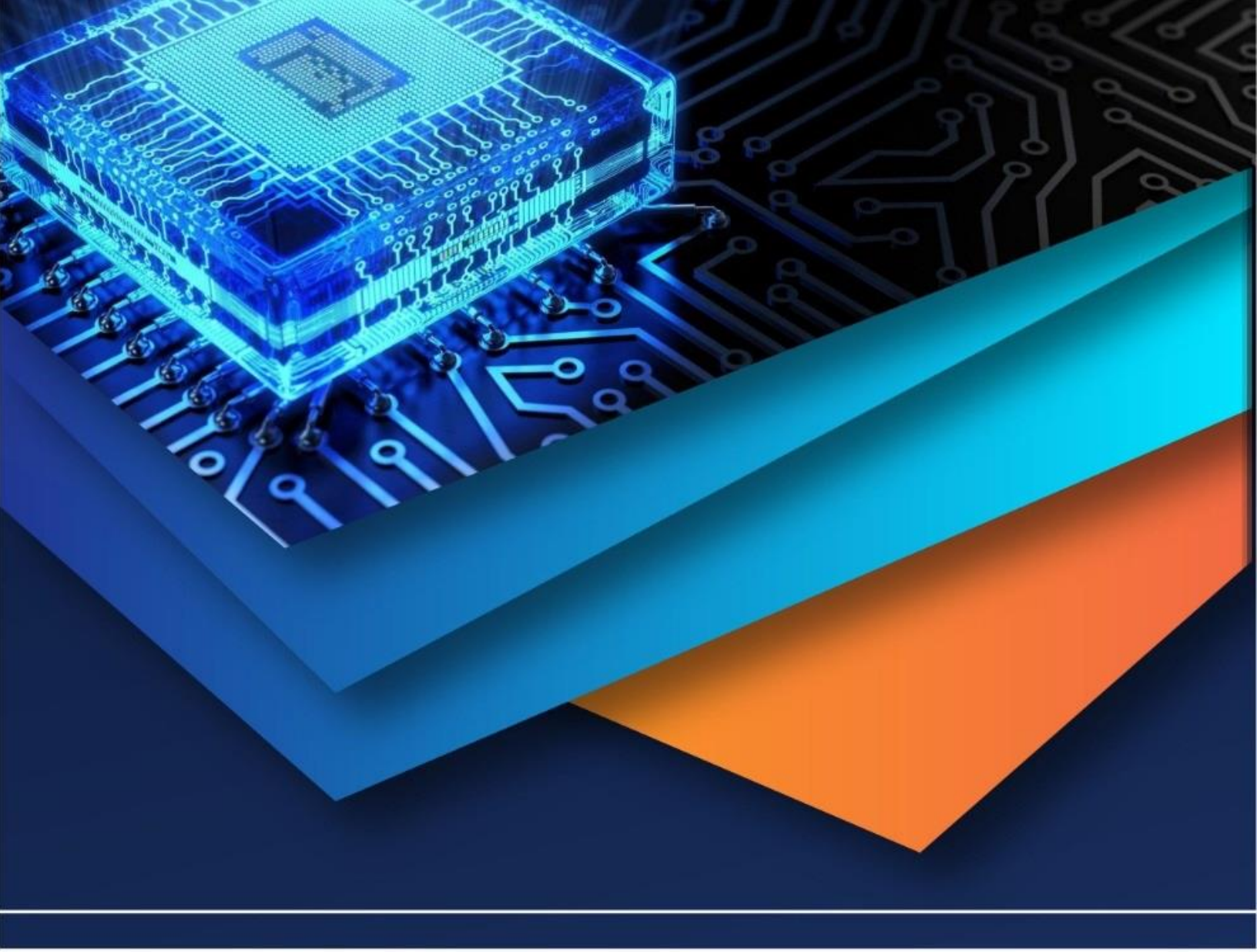
Flow Status	Successful - Sun Apr 02 16:26:25 2017
Quartus II Version	9.0 Build 132 02/25/2009 SJ Web Edition
Revision Name	UU
Top-level Entity Name	CODEC_MODULE
Family	Cyclone III
Met timing requirements	N/A
Total logic elements	12,006 / 24,624 (49 %)
Total combinational functions	11,295 / 24,624 (46 %)
Dedicated logic registers	4,277 / 24,624 (17 %)
Total registers	4277
Total pins	134 / 216 (62 %)
Total virtual pins	0
Total memory bits	0 / 608,256 (0 %)
Embedded Multiplier 9-bit elements	4 / 132 (3 %)
Total PLLs	0 / 4 (0 %)
Device	EP3C25F324C6

VI. CONCLUSION

In this paper ,it is proved that the robustness of transformed domain watrmarking concept with Cryptography including the various schemes of system based on the kind of key and a few algorithms such as DCT and RC5. The mathematical foundations for RC5 based systems, and possibilties of DCT macro block conversion and its physical domain transformation properties are studied. And finally the computational and security metrics of DCT is proved and their complexity reduction were also analyzed using FPGA hardware synthesis.

REFERENCES

[1] SA. Lumini and D. Maio (2000), A Wavelet-Based Image Watermarking Scheme, The International Conference on Information Technology: Coding and Computing, Las Vages, NV, pp. 122-127.
[2] Amit Joshi, Vivekanand Mishra (2011), Blind video watermarking of wavelet domain for copy right protection ,International Journal of Computing, Vol 1, Issue 3,pp 291-295.
[3] Amit Joshi, Prof.A.D.Darji (2009), Efficient Dual Domain Watermarking for secure images, An International Conference on dvances in Recent Technologies in Communication and Computing, 2009. ARTCom '09, pp. 909-914.
[4] Arun Kejariwal (2003), Watermarking, IEEE Potential, October/November, 2003.pp 37-40. B. Sehneier (1996), Applied Cryptography: Protocols, Algorithms and Source Code in C, second edition, John Wiley & Sons, New York.
[5] Dekun Zou, Jeffrey A. Bloom(2008): H.264/AVC stream replacement technique for video watermarking. ICASSP 2008: 1749-1752
[6] Frank Hartung, Bernod Girod(1998),"Watermarking of uncompressed and compressed domain Video",Elseiver,Vol 66,no. 3,May 1998,pp 283-301
[7] Garimella, A., Satyanarayan, M.V.V., Kumar, R.S., Murugesh, P.S., Niranjan (2003) ,VLSI Implementation of Online Digital Watermarking Techniques with Difference Encoding for the 8-bit Gray Scale Images In: Proc. of the Intl. Conf.on VLSI Design.,pp 283–288
[8] Hyun Lim, Soon-Young Park and Seong jun Kang (2003), FPGA Implementation of Image Watermarking Algorithm for a Digital camera, IEEE Pacific Rim Conference on Communications, Computers and signal Processing, 2003. PACRIM. 2003, pp.1000-1003.
[9] Hsien-Wen Tseng , Chin-Chen Chang (2008), An extended difference expansion algorithm for reversible watermarking ,Elsiver, Image and vision computing, pp 1148-1308
[10] I .J. Cox, J. Kilian, T. Leighton and T. Shanon (1995), Secure spread spectrum for Multimedia, NEC research institute, prinecton, NJ, technical report pp. 95-10.
[11] I.J.Cox,J. Kilian, F.T. Leighton, and T. Shamoon (1997), Secure Spread Spectrum Watermarking for Multimedia, IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY