Adaptive Cryptosystem for Digital Images using Fibonacci Bit-Plane Decomposition

Ravindranath C. C
EX Dept., GGITM
Raisen Road, Anand Nagar
Bhopal, MP-462021

Aditya Kumar Bhatt
EX Dept., GGITM
Raisen Road, Anand Nagar
Bhopal, MP-462021

Aditi Bhatt
NCRA., TIFR
H-10, NCRA Hostel
Pune, MH-411007

ABSTRACT
In this paper, we introduce a novel encryption algorithm based on Fibonacci numbers. In addition, novel bit-plane decomposition for Fibonacci weights is also discussed that offers cryptographic benefits. The new lossless image encryption algorithm is presented can encrypt an image using this new decomposition method for privacy protection. Further, it has two levels of encryption that could address both pay-per-view applications or secured communication simultaneously. Simulation results and analysis verify that the algorithm shows good performance in image encryption.

General Terms
Image Scrambling, Security, Secured Communication

Keywords
Image scrambling, encryption, fibonacci bit-plane decomposition, secured communication

1. INTRODUCTION

In the current digital era, the rapid escalations in digital multimedia and network have paved ways for people around to acquire, utilize and share multimedia information. The need for intellectual property right protection has become a new research area involving statistics, cryptography, information hiding, and computer vision as some of the techniques [1]. Since, the information that could benefit or educate groups (or individual) can also be used against such groups (or individual). Hence forth, the information security has evolved as an important and urgent issue not only for individuals but also for business and governments. Digital image & video scrambling has evolved as a hot topic among the researchers of digital data security.

Cryptography is science that protects data by transforming it into a digital form which is not discernible to an attacker without the secret key [2]. A perfect image cryptosystem is not only flexible in the security mechanism, but also has high overall performance. Thus, besides the above characteristics, the image security also needs to address the following problems [3]:

1. Encryption system should be computationally secure. It must require an extremely long computation time to break, for example. Unauthorized users should not be able to read privileged images.

2. Encryption and decryption should be fast enough not to degrade system performance. The algorithms for encryption and decryption must be simple enough to be done by users with a personal computer.

3. Minimal distortion between the decrypted image and original image.

4. Security mechanism should be flexible.

5. Security mechanism should be as widespread as possible. It must be widely acceptable to design a cryptosystem like a commercial product.

L. Chuanmu. et.al. [4] proposed a secured image encryption method based on the hyper chaotic map to meet the constraints of secured multimedia transfer system. The basic principle of this method is the permutation of the pixel location within the image decided by a chaotic map generated from a chaotic pseudo random binary sequence. F. Hani Ali et.al [5] propose the use of cyclic shift and bit wise XOR operation as new approach to replace the lookup table. The principle benefit of using this new approach over the transform from Rijndael block cipher is speed. Y. Zhou. et.al. [6] introduces two new multimedia scrambling algorithms based on the P-recursive sequence. The algorithms can be used to scramble two or three dimensional multimedia data in one step. Furthermore, a security key parameter p may be chosen as different or the same values providing partially or fully encrypting multimedia data. Generalized Fibonacci transformations with application to image scrambling are presented in detail by authors in [7-9].

The remainder of this paper is organized as follows. In Section 2, we introduce the existing Fibonacci based decomposition and propose a novel decomposition method. Section 3 introduces the new approach formula where traditional cyclic shift been replaced by constraint based cyclic shift methodology. Section 4 deals with proposed system framework and the basic steps involved. Section 5, presents the simulations results associated with proposed algorithm. The conclusion of the paper is presented in the section 6.

2. FIBONACCI BIT-PLANES

Digital imagery is commonly found in 8-bit format, grayscale or indexed images (i.e. PNG, GIF) as well as in 24-bit true color format (i.e. BMP, TIF), which is a combination of three 8-bit color layers. The 8-bit format is widely used for its conformity with memory configuration in hardware and the efficiency of the binary standard formulated by the Euclidian algorithm. A string of 8 binary values is multiplied with a sequence containing the first 8 powers of 2 i.e. {1, 2, 4, 8, 16, 32, 64, 128}. The resultant products are then summed together to calculate the represented pixel value.

One way to design a robust algorithm is to find an alternate representation of the pixel value that could offer cryptographic benefits. In addition, we discuss by a novel encryption algorithm based on localized cyclic shift based image scrambling system.

2.1 Fibonacci Number Set

Fibonacci numbers are a sequence of values that are generated using a fixed pattern. The values in these number sequences are smaller than those found in the typical number power of two's, thus requiring a binary string longer than eight in order to allow representation of pixel values up to 255 [10]. Fibonacci codes may be defined as follows.

$$f(i) = \begin{cases} 0 & i < 0 \\ 1 & i = 0 \\ f(i-1) + f(i-2) & i > 0 \end{cases} \quad .. \quad (1)$$

The sequences displayed give the exact number of values that are necessary in order to represent pixel values in the range of [0,255] i.e., [1,1,2,3,5,8,13,21,34,55,89,144, 233]. The natural number *A* may be expressed using the number F(i)

$$A = \sum_{i=0}^{n-1} a_i F(i) \quad \text{... (2)}$$

Where the string $a_i \in \{0,1\}$, there is a correspondence between *A* and sequence code. The string a_i, having a length of *n*, represents *A* in the form

$$A \leftrightarrow (a_0, a_1, a_2, \ldots, a_{n-2}, a_{n-1}) \quad \ldots (3)$$

But this correspondence is not unique as there are numerous possibilities. For example, the number 40 has the following different combinations for a given Fibonacci sequence.

40 = [1 0 0 0 1 0 0 0 1 0 0 0 0]$_{2f}$ = [0 1 0 0 1 0 0 0 1 0 0 0 0]$_{2f}$

= [1 0 0 0 1 0 1 1 0 0 0 0 0]$_{2f}$ = [0 1 0 0 1 0 1 1 0 0 0 0 0]$_{2f}$

= [1 0 1 1 0 0 1 1 0 0 0 0 0]$_{2f}$ = [0 1 1 1 0 0 1 1 0 0 0 0 0]$_{2f}$

= [1 0 1 1 1 1 0 1 0 0 0 0 0]$_{2f}$ = [0 1 1 1 1 1 0 1 0 0 0 0 0]$_{2f}$

= [1 0 1 1 0 0 0 0 1 0 0 0 0]$_{2f}$ = [0 1 1 1 0 0 0 1 0 0 0 0 0]$_{2f}$

From the above example, it is evident that a unique normalized representation for Fibonacci number sets is vital for security based applications. Dey. S [10 - 11] designed a set of dictionary of unique representation for pixel values between [0 - 255] based on Zeckendorf's theorem to overcome the unique representation issue. Unfortunately, the receiver requires the prior knowledge of unique representation dictionary set for lossless recovery of the encrypted data. Hence to design a lossless encryption system, we need a novel data modeling operator so that we could eliminate the use of dictionary set at the receiver.

2.2 Normalized Fibonacci Set

Most of the common normalized decompositions based on the Fibonacci numbers set is based on Zeckendorf's theorem [12]. **Zeckendorf's theorem** states that every positive integer can be represented uniquely as the sum of *one or more* distinct Fibonacci numbers in such a way that the sum does not include any two consecutive Fibonacci numbers. Thus based on the Zeckendorf's theorem the possible combinations for the number 40 are

40 = [**1 0 0 0 1 0 0 0 1 0 0 0 0**]$_{2f}$ [**0 1 0 0 1 0 0 0 1 0 0 0 0**]$_{2f}$

Further to attain a normalized decomposition, monotonic Fibonacci weights (i.e. {1,2,3,5,8,13,21,34,55,89,144,233}) are considered that would yield normalized Fibonacci decomposition as follows

40 = [**∅ 1 0 0 1 0 0 0 1 0 0 0 0**]$_{2f}$ ↔ [**1 0 0 1 0 0 0 1 0 0 0 0**]$_{2f}$

This decomposition provides normalized representation, but we could identify the need of new and novel unique normalized representation system for encryption method to enhance cryptographic benefits. This notion motivated us to investigate various coding techniques and develop a novel normalized representation that helps us in various image processing applications. Further this frame would enhance the cryptographic benefits of the proposed scheme as the size of the key would increase.

2.3 Proposed Normalized Fibonacci Set

In this section, we introduce a novel unique normalized representation system for Fibonacci weights.

Theorem 1[13]: *Any natural number can be uniquely represented by set of Fibonacci weights based on the following representation*

For Max representation: $\underbrace{max}_{rep} \left\{ \sum_{i=0}^{n-1} 2^i * a_j \right\}$ … (4)

For Min representation: $\underbrace{min}_{rep} \left\{ \sum_{i=0}^{n-1} 2^i * a_j \right\}$ … (5)

Where, a_j is the one the j representations possible for a pixel value in the number system, "n" indicates the length of representations, and $\max_{rep}$ / $\min_{rep}$ is the maximum or minimum value associated with Euclidean distance of the representation.

Normalized Fibonacci decomposition based on proposed theorem would yield the following for the number 40:

40 = [0 1 0 0 1 0 0 0 1 0 0 0 0]$_{fmax}$

= [1 0 1 1 1 1 0 1 0 0 0 0 0] $_{fmin}$ for non monotonic weights

= [0 1 1 1 1 1 0 1 0 0 0 0 0] $_{fmin}$ for monotonic weights

The bit-plane decomposition of the images can be best explained based on the image representation. Figure 1, illustrates the red layer decomposition of the cover image based on the Max Fibonacci decomposition (fmax). Figure 2, illustrates the red layer decomposition of the cover image

based on the Min Fibonacci decomposition (fmin) for monotonic weights.

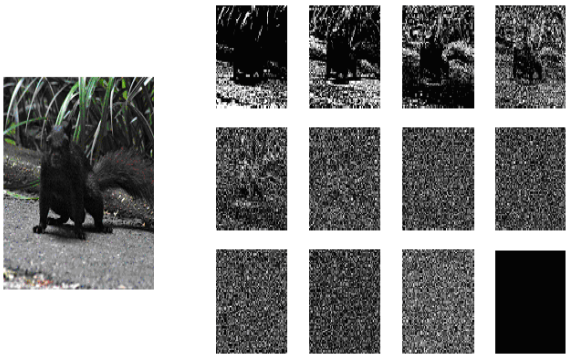


Figure 1. Bit-plane decomposition using the max Fibonacci weights

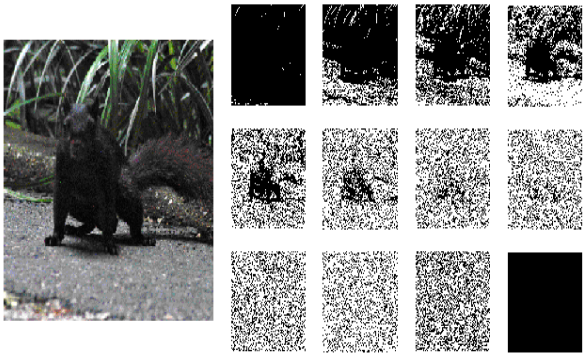


Figure 2. Bit-plane decomposition using the min Fibonacci weights

3. CYCLIC SHIFT

A cyclic shift is the operation of rearranging the entries in a tuple, either by moving the final entry to the first position, while shifting all other entries to the next position, or by performing the inverse operation. Circular shifts are used often in cryptography in order to permute bit sequences of the data. The cyclic shift operation over the Fibonacci bit-planes can be better understood using Table 1. From Table 1, it is evident that the regular cyclic shift could not be applied over the Fibonacci based sequences as they would results in irradiant sequences i.e.

- Either sum of the shift sequence would yield a value outside the range of [0 - 255] Or
- Either the shift sequence would not validate the normalized constraints.

Hence to overcome these issues, we propose a constraint based cyclic shift that could be effective employed in the framework. Further it would also provide cryptographic benefits to the proposed system.

TABLE 1
CYCLIC SHIFT VALUE FOR 239 BASED ON FMAX

Shift code	Cyclic Shift Sequence	Value
0	[0 1 0 0 1 0 0 0 0 0 0 0 1]	239
1	[1 0 1 0 0 1 0 0 0 0 0 0 0]	11
3	[0 0 1 0 1 0 0 1 0 0 0 0 0]	28
4	[0 0 0 1 0 1 0 0 1 0 0 0 0]	45
7	[0 0 0 0 0 0 1 0 1 0 0 1 0]	191
9	[1 0 0 0 0 0 0 0 1 0 1 0 0]	124
11	[0 0 1 0 0 0 0 0 0 0 1 0 1]	324

3.1 Constrained Cyclic Shift

In this section, we introduce a novel cyclic shift framework based on constraints that could address the issues discusses earlier. The proposed constraints that are induced over the cyclic shift are as follows

1. a_1 is always zero, thus monotonic Fibonacci weights are considered
2. If $a_1 = a_{12} =$, then two coefficients are shifted in cyclic order. This ensures the shifted sequence is within the normalized constraints.
3. If the Shift value outside the range [0 -255] then the shift is skipped to the next shift. This ensures the value of the shifted sequence is within the range

These constraints will create ambiguousness within the decryption algorithm, thus proper decoding key is essential for retrieving the information. The constraint based cyclic shift operation over the Fibonacci bit-planes can be better understood using Table II.

TABLE 1I
CYCLIC SHIFT VALUE FOR 239 BASED ON FMAX

Shift code	Cyclic Shift Sequence	Value
0	[0 1 0 0 1 0 0 0 0 0 0 0 1]	239
1	[0 1 0 1 0 0 1 0 0 0 0 0 0]	17
3	[0 0 0 1 0 1 0 0 1 0 0 0 0]	45
4	[0 0 0 0 1 0 1 0 0 1 0 0 0]	52
7	[0 1 0 0 0 0 0 0 0 1 0 1 0]	200
9	[0 1 0 0 1 0 0 0 0 0 0 0 1]	239
11	[0 0 1 0 1 0 0 1 0 0 0 0 0]	28

4. Proposed System

In this section, we introduce a novel encryption algorithm based on Fibonacci numbers that incorporates the concepts discussed in the earlier sections. The general structure of the encryption process is presented in the Figure 3.

The basic components of the proposed encryption framework are presented as follows

Inputs: - *Cover Image.* The cover image may be of any image format using the 8-bit, power of two's representation. The proposed algorithm may also be applied on 24-bit, each color layer images treated as an individual 8-bit image.

Fibonacci Weights. Monotonic Fibonacci numbers are used as bit-plane weights. These sequence numbers can be replaced by any non redundant natural numbers weights.

System I: - *Pre-processing System.* This system consists of following components i.e. pixel pre-processing block, proposed representation block (Fmax or Fmin) and corresponding bit-plane decomposition. This system could take any digital media (images, binary data & etc) can pre-process to get pixel value (range 0-255) and decompose based on Fmax, Fmin representation. The mode of representation and weights employed would be transformed as a key to stored, for successful reconstruction of the encrypted image (without loss of integrity or quality).

System II: - *Encryption System*. This consists of the following components i.e. encryption process and cyclic shift constraints. In this paper, we focus on the cyclic shift as the encryption process to illustrate its effects on Fibonacci based decomposition. From section III, we realized that a simple cyclic shift operation would not result is lossless encryption approach. Hence to realize and maintain the lossless nature of the encryption algorithm, we introduce constraints on the cyclic shift.

Outputs: - *Crypto Image and Crypto Key.*

The decryption process is a straightforward process where all necessary parameters are dictated based on the crypto-key. Cover image is reconstructed without any loss or integrity from the encrypted image given as input.

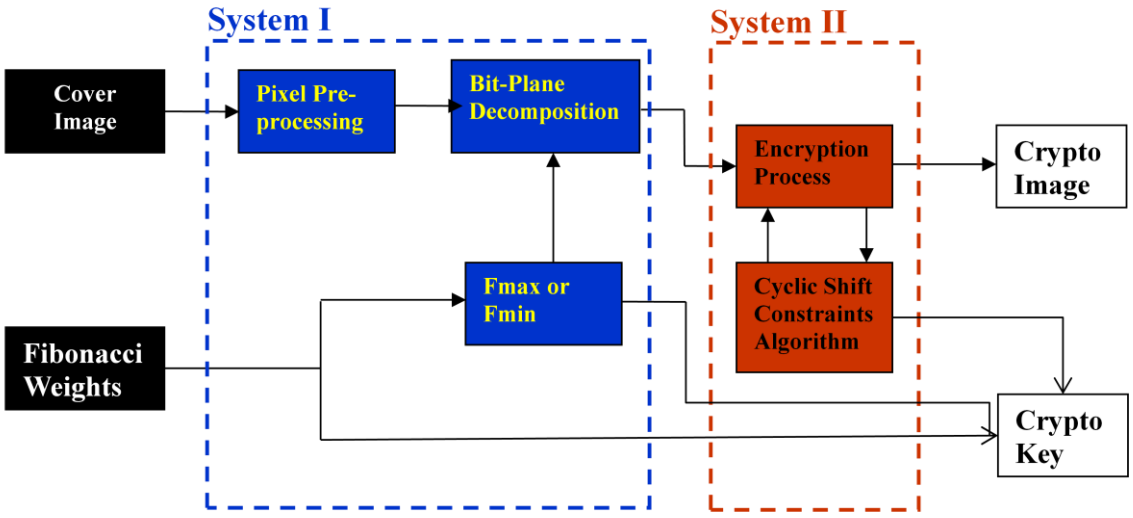


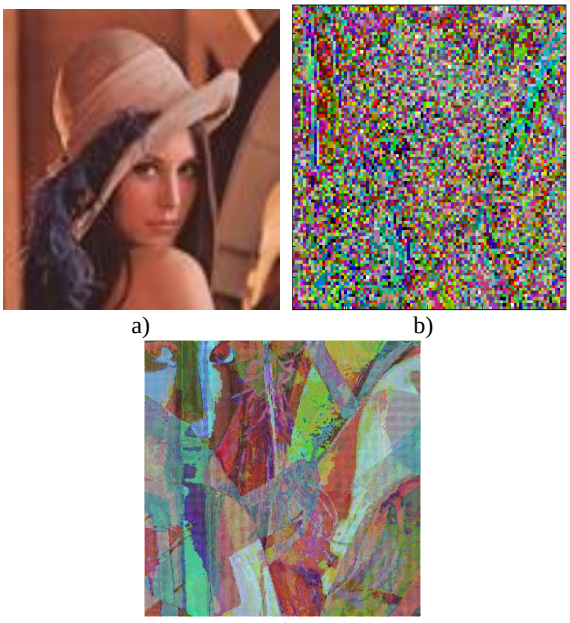
Figure 3. The general structure of the encryption process

5. COMPUTER SIMULATIONS

In this section, the simulations results of proposed security system are presented. Computer simulations were simulated using MATLAB software package. Analysis was done using 100 color images of varying sizes, texture and contour (simulations are presented for 5 images). These images were taken using 2 digital cameras Nikon D100 and Canon EOS Digital Rebel and modified in Photoshop to attain a smooth histogram.

Initial investigation to test robustness, was based on the visual randomness of the encrypted images from the original image in consideration. Figure 4, shows the visual randomness of the cover image after a cyclic shift (code = 3) fmax and a cyclic shift (code = 5) fmax.

Table III, shows the percentage pixel change in each layer of "Lena" image for all the possible shift codes. In addition, shift code '4' shows maximum distortion between the cover and encrypted image on average of the three layers. Figure 5, introduces the histogram comparison for various shift codes (i.e. 4, 6, 8) over the "Sarkis" image using proposed encryption algorithm. Table IV, shows the percentage pixel change in each bit-plane of "Lena" & "Sarkis" image for shift code '4'.



a) b)

c)

Figure 4. a) Original image b) Encrypted via cyclic shift (code = 3) c) Encrypted via cyclic shift (code = 5)

TABLE III
Percentage Pixel change in each layer of Lena for each Shift code

Shift Code	R	G	B
1	50.866	68.5615	65.5436
2	69.1407	75.3127	68.5037
3	83.5613	89.4482	72.4209
4	86.4494	88.8537	75.8502
5	79.7377	83.8537	81.6119
6	71.5777	79.0445	87.9407
7	59.9112	75.0346	81.5545
8	58.5200	77.0777	79.0613
9	59.1331	77.8064	76.6423
10	64.8669	83.3201	79.3222
11	75.6144	87.6402	84.9092

TABLE IV
Percentage change in the for each bit-plane for both images

Bit planes	Lena	Sarkis
1	92.61	94.72
2	92.79	95.74
3	93.24	94.95
4	93.04	95.04
5	93.47	95.15
6	93.36	95.60
7	94.22	95.26
8	100	99.67

Furthermore, the attacker may employ the brute-force attack that tries all possible permutations to construct the perfect master share for a protected image. If the protected image of size 512x512 pixels, the number of required trials to construct the perfect master is $2^{512\times512}$, that is computationally infeasible for current computers.

6. CONCLUSION

In this paper, we introduced a novel encryption algorithm based on Fibonacci numbers. In addition, novel bit-plane decomposition for Fibonacci weights was also discussed that offers cryptographic benefits to the proposed system. This lossless image encryption algorithm can employed for privacy protection and could address both pay-per-view applications or secured communication simultaneously. Simulation results and analysis verified that the algorithm shows good performance in image encryption.

7. REFERENCES

[1] D. Schneier, *Applied Cryptography*, John Wiley & Son, Inc., New York, NY, 1996

[2] A.M. Eskicioglu, "Multimedia Security in Group Communications: Recent Progress in key management, authentication, and watermarking", *Multimedia Systems*, vol. 9, no. 3, Springer-Verlag Berlin/Heidelberg, pp. 239 – 248, 2003

[3] B. Furht, D. Socek, and A.M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques," Chapter in Multimedia Security Handbook, pp. 94 – 144, CRC Press, 2005

[4] L. Chuanmu and H. Lianxi, "A new image encryption scheme based on hyper chaotic sequences", IEEE International Workshop on Anti-counterfeiting, Security, Identification, 16-18 April 2007, pp.237 – 240

[5] Fakariah Hani Mohd Ali, Ramlan Mahmod, Mohammad Rushdan and Ismail Abdullah, "A Faster Version of Rijndael Cryptographic Algorithm Using Cyclic Shift and Bit Wise Operations", International Journal of Cryptology Research pp: 215-223 (2009).

[6] Yicong Zhou; Panetta, K.; Agaian, S.; "An image scrambling algorithm using parameter bases M-sequences", International Conference on Machine Learning and Cybernetics, Vol 7, July 2008 pp:3695 – 3698

[7] Yicong Zhou, Karen Panetta, Ravindranath Cherukuri and Sos Agaian, "Selective object encryption for privacy protection", Proc. SPIE 7351, 73510F (2009); doi:10.1117/12.817699

[8] Jiancheng Zou; Ward, R.K.; Dongxu Qi; "The generalized Fibonacci transformations and application to image scrambling", IEEE International Conference on Acoustics, Speech, and Signal Processing, Vol 3, 17-21 May 2004, pp 385-388.

[9] Jiancheng Zou; Ward, R.K.; Dongxu Qi; "A new digital image scrambling method based on Fibonacci numbers", International Symposium on Circuits and Systems, ISCAS '04, Vol 3, 23-26 May 2004, pp:III - 965-8.

[10] Dey. S., Abraham. A., Sanyal. S, "An LSB data hiding technique using prime numbers", Third international symposium on Information assurance and security, pp 101-108, (2007).

[11] Dey. S., Abraham. A., Sanyal. S, "An LSB data hiding technique using natural numbers decomposition", Third international conference on Intelligent information Hiding and Multimedia Signal Processing, vol.2, pp 473-476, (2007).

[12] Basin, S. L. and Hoggatt, V. E. Jr. "A primer on the Fibonacci Sequence", Fib. Qurat. 1, 1963

[13] Ravindranath C. Cherukuri and Sos S. Agaian, "New normalized expansions for redundant number systems: adaptive data hiding techniques", Proc. SPIE 7542, 754206 (2010); doi:10.1117/12.