A Scheme for Secure Transmission of Multiple Images using MCKBA and FFWPDM

P. V. Murali Krishna¹, G. Sahu², and D. Arun Kumar³

¹,²,³Assistant Professor, Department of Electronics & Communication Engineering, GMRIT, Rajam, INDIA

ABSTRACT

Chaos based encryption may offer new quality in secure data transmission. A recently proposed chaotic-key based algorithm (CKBA) has been shown to be unavoidably susceptible to chosen/known-plaintext attacks and ciphertext-only attacks. In this paper, a new algorithm based on modified chaotic-key based algorithm (MCKBA) and finite field wavelet packet division multiplexing (FFWPDM) is proposed for secure orthogonal multiplexing of images.

Keywords: chaos, cryptography, image encryption, image decryption, wavelet packet division multiplexing

I. INTRODUCTION

The advances in communication technology have seen strong interest in digital signal transmission. However, illegal data access has become more easy and prevalent in wireless and general communication networks. Because of their sensitivity to initial conditions and control parameters, chaotic signals have been used in data encryption [1-5].

In the new chaotic key-based algorithm (CKBA) [1], according to a binary sequence generated from a chaotic system, the gray level of each pixel is XORed or XNORed bit-by-bit to one of the two predetermined keys. The CKBA is simple and attractive with the decryption procedure just like encryption. However, it is proved in [6] that the CKBA is very weak to the chosen/known plain text attack when the same key is used to encrypt more than one image. Further, an improvement to CKBA based on increasing the key sizes is proposed in [6], this only improves the resistance to a cipher text attack only and does nothing to prevent known/known plain text attacks. Based on the increased key sizes and piecewise linear chaotic map, an algorithm is reported in [5] to enhance CKBA. A modified chaotic key based algorithm (MCKBA) with increased key size is developed in [7] for improved security. And a new algorithm based on chaos and Brahmagupta–Bhāskara (BB) equation is developed in [8] for image encryption and decryption with moderate size of keys.

Wavelet packet-division multiplexing (WPDM) is a high-capacity, flexible, and robust multiple-signal transmission technique in which the properties of wavelet packet basis functions are used for orthogonal multiplexing. Finite field wavelet packet-division multiplexing (FFWPDM) provides orthogonal multiplexing of the images and encrypt the images. Finite field Wavelet packet-division multiplexing convert the input images data to a sequence similar to white noise. Hence in this paper a new algorithm is proposed for secure transmultiplexer for images using MCKBA and finite field wavelet packet-division multiplexing (FFWPDM).

II. METHODS AND MATERIAL

2.1 Finite Field Discrete Wavelet Transform

The wavelet system can be implemented using a two-band analysis-synthesis filter bank. Fig. 1 shows the analysis and synthesis banks of a two-channel perfect reconstruction filter bank. More specifically, the analysis bank performs the wavelet transform and the synthesis bank performs the inverse wavelet transform. X(n) is the input data and the sequences labeled y₀(n), y₁(n) are the wavelet coefficients.
Let \( H_s(z) \), \( G_s(z) \) where \( s = 0, 1 \), be the polynomial representation of the filters \( h_s(n) \), \( g_s(n) \) in Fig. 1. Suppose that these polynomials have order \( 2N+1 \) with poly phase components \( E_s(z), E_s(z), R_s(z) \) and \( R_s(z) \) so that

\[
H_s(z) = E_s(z^i) + z^{-i}E_s(z^i) \\
G_s(z) = z^{-i}R_s(z^i) + R_s(z^i)
\]

(1)

(2)

Using the poly phase representation for the two-band orthogonal filter banks, the following can be deduced:

\[
H_s(z) = -z^{(2N+1)}H_s(-z^{-1}), \\
G_s(z) = H_s(-z), G_s(z) = -H_s(-z)
\]

(3)

Any two polynomials \( A(Z) \) and \( B(Z) \) over a Galois field \( F(Z) \) that satisfy the polynomial equation

\[
A(z)A'(z) + B'(z)B(z) = Z^u
\]

(4)

can be used to generate the coefficients of wavelet filter banks. The polynomials \( A(Z) \) and \( B(Z) \) over a Galois field \( F(Z) \) are defined as

\[
A(z) = \sum a_i z^i, a_i \neq 0, \quad B(z) = \sum b_j z^j, b_j \neq 0, \quad a, b \in GF(p')
\]

(5)

where \( M \) is a positive integer satisfying \( M < N \).

In our notation, the superscript “c” means the reciprocal of the polynomial. The reciprocal of a polynomial \( q(z) \) of degree \( M \) is defined as \( q'(z) = z^M q(z^{-1}) \).

The coefficients of the two polynomials \( A(Z) \) and \( B(z) \) are related to the poly phase components \( E_s(z) \) and \( E_s(z) \) by

\[
E_s(z) = A(z^{-i}), \quad E_s(z) = z^{i+M}B(z^{-i})
\]

(6)

The M channel transmultiplexer is shown fig. 2a. Finite field two-band orthogonal filter banks are used to construct a finite field wavelet packet-division multiplexing (FFWPDM) transmultiplexer for four-users which is shown fig 2b.

2.2 The Proposed Secure Transmultiplexer Algorithms Based on Chaos and FFWPDM

The chaotic function that used is the well-known logistic map given by

\[
x(i + 1) = \mu x(i)(1 - x(i))
\]

(7)

where \( \mu = 3.9 \). Let \( g \) denote an image of size \( M \times N \) pixels and \( f(x, y) \), \( 0 \leq x \leq M -1, 0 \leq y \leq N -1 \), be the gray level \( f \) at position \( (x, y) \).

A. The Proposed MCKBA -FFWPDM for multiplexer

The MCKBA for encryption is as follows.

Step 1: choose \( \text{key1} \) and \( \text{key2} \) and set \( j=0 \)

Step 2: Choose the initial point \( x(0) \) and generate the chaotic sequence \( x(0), x(1), x(2), ... \), \( (MN/16-1) \) using eq.(1) and then create \( b(0), b(1), b(2), ..., b(2MN-1) \) from \( x(0), x(1), x(2), ... \), \( (MN/16-1) \) by the generating scheme such that \( b(32i+0) \), \( b(32i+1) \), ..., \( b(32i+29) \), \( b(32i+30) \) \( b(32i+31) \) is the binary representation of \( x(i) \) for \( i = 0, 1, 2, ... \), \( (MN/16-1) \).

Step 3: For \( x=0 \) to \( M-1 \)

For \( y = 0 \) to \( N-1 \)

Switch \( (2x b(j) + b(j+1)) \)

Case 3: \( f_e(x, y) = \text{mod} ((f(x, y)+\text{key1}), 2^{n-1}) \)

\( f_e(x, y) = f_e(x, y) \text{ XOR key1} \)

Case 2: \( f_e(x, y) = \text{mod} ((f(x, y)+\text{key1}), 2^{n-1}) \)

\( f_e(x, y) = f_e(x, y) \text{ XNOR key1} \)

Case 1: \( f_e(x, y) = \text{mod} ((f(x, y)+\text{key2}), 2^{n-1}) \)

\( f_e(x, y) = f_e(x, y) \text{ XOR key2} \)

Case 0: \( f_e(x, y) = \text{mod} ((f(x, y)+\text{key2}), 2^{n-1}) \)

\( f_e(x, y) = f_e(x, y) \text{ XNOR key2} \)

\( = j+2; \)

End; End

Step 4: apply the above steps for images \( f_1, f_2, f_3 \) and \( f_4 \) and obtain \( f_{e1}, f_{e2}, f_{e3} \) and \( f_{e4} \).

Step 5: apply the \( f_{e1}, f_{e2}, f_{e3} \) and \( f_{e4} \) to FFWPDM multiplexer to obtain \( F \).

B. The Proposed MCKBA -FFWPDM for demultiplexer

Step 1: apply the \( F \) to FFWPDM demultiplexer to obtain \( f_{e1}, f_{e2}, f_{e3} \) and \( f_{e4} \).

Step 2: choose \( \text{key1} \) and \( \text{key2} \) and set \( j=0 \)
**Step 3:** Choose the initial point x(0) and generate the chaotic sequence x(0), x(1), x(2),..., x(MN/16-1) using eq.(1) and then create b(0), b(1), b(2),...., b(2MN-1) from x(0), x(1), x(2),..., x(MN/16 -1) by the generating scheme such that b(32i+0) b(32i+1) b(32i+2) b(32i+3) b(32i+4) b(32i+5) is the binary representation of x(i) for i = 0, 1, 2,... (MN/16-1)

**Step 4:** For x=0 to M-1
For y = 0 to N-1
Switch (2×b(j) + b(j+1))
  case 3:  \( f(x,y) = f_e(x,y) \oplus \text{key1} \)
  \( f(x,y) = \text{mod}((f(x,y) - \text{key1}),2^{n-1}) \)
  case 2:  \( f(x,y) = f_e(x,y) \oplus \text{key1} \)
  \( f(x,y) = \text{mod}((f(x,y) - \text{key1}),2^{n-1}) \)
  case 1:  \( f(x,y) = f_e(x,y) \oplus \text{key2} \)
  \( f(x,y) = \text{mod}((f(x,y) - \text{key2}),2^{n-1}) \)
  case 0: \( f(x,y) = f_e(x,y) \ominus \text{key2} \)
  \( f(x,y) = \text{mod}((f(x,y) - \text{key2}),2^{n-1}) \)
  \( j = j + 2; \)
End; End

**Step 5:** Apply the above steps 2 to 4 for images \( f_{e1}, f_{e2}, f_{e3} \) and \( f_{e4} \) to obtain \( f_1, f_2, f_3 \) and \( f_4 \).

The ‘mod’ stands for modulus after division.

Because not all secret keys can make well disorderly encrypted images, the basic criterion to select key1 and key2 should satisfy \( \sum_{i=0}^{n-1} (a_i \oplus d_i) = n/2, \)

key1 = \( \sum_{i=0}^{n-1} a_i \times 2^i \) and key2 = \( \sum_{i=0}^{n-1} d_i \times 2^i \), n is bit length of key1 and key2

**III. RESULTS AND DISCUSSION**

**SIMULATION RESULTS**

The secure transmultiplexer for four users is implemented using MCKBA -FFWPDM on the 8 bits per pixel 256X256 Girl(LENA),Cameraman, goldenear and IC images in GF(2^{18}). The original Girl(LENA),Cameraman, goldenear and IC images are shown in Fig. 8(a). In the implementation of secure transmultiplexer using MCKBA -FFWPDM, 16 bit keys are used. The key1 and key2 are set to key1 = 36408 (10001110001110002) and key2 = 61499 (11110000001110112) and \( \mu = 3.9 \), x (0) =0.75, are used for the logistic maps. The floating point arithmetic is used for logistic map. The filter banks are constructed over GF (2^{18}) with the primitive polynomial \( q(x) = x^8 + x^7 + 1 \). The polynomials and \( B(z) = 131014 + z^{-1} \) are used. The corresponding poly phase components are \( E^{(z)}_0 = 131009 + 7z^{-1} \), \( E^{(z)}_1 = 131014 + z^{-1} \)

The multiplexed image obtained using secure transmultiplexer using MCKBA -FFWPDM is shown in Fig. 8(b). From Fig. 8(b), it can be observed that the secure transmultiplexer using MCKBA -FFWPDM has created highly disordered image of the original images. The demultiplexed images using secure transmultiplexer using MCKBA -FFWPDM are same as original images as FFWPDM is lossless transform.
Fig. 2a: Four user FFWPDM synthesis bank (Multiplexer)

Fig. 3: Cascade architecture of EU and FFWPDM Multiplexer

Fig. 4: Architecture of Encryption Unit

Fig. 5: Architecture of FFWPDM synthesis lowpass filter and high pass filter

Fig. 6: Cascade architecture of FFWPDM demultiplexer and DU

Fig. 7a: Architecture of FFWPDM analysis low pass filter

Fig. 7b: Architecture of FFWPDM analysis high pass filter

Fig. 8a: Original image: Lena, cameraman, gloves and SC

Fig. 8b: Multiplexed image using MCM3A-FFWPM/Multiplexer
IV. CONCLUSION

In this paper, a secure transmultiplexer for images using modified chaotic key-Based algorithm and finite field wavelet packet-division multiplexing (MCKBA–FFWPDM) with moderate size of keys is proposed. It gives more security to data.

V. REFERENCES


