A Novel Method for Secure Image Delivery over Mobile Networks Based on Orthogonal Transforms and Scrambling Algorithms

Mohammad V. Malakooti [(1)], Vahid Saffari [(2)], Tawfik Saeed Zeki [(3)]

(1) Faculty and Head of Department of Computer Engineering, Islamic Azad University, UAE Branch, Dubai, UAE
malakooti@iau.ae

(2) Graduate Student of Department of Computer Engineering, Islamic Azad University, UAE Branch, Dubai, UAE
saffari@iaushiraz.ac.ir

(3) Faculty of Department of Computer Engineering, Islamic Azad University, UAE Branch, Dubai, UAE
Tawfik@iau.ae

Abstract: We have presented a novel method for secure image delivery over the mobile networks. Our method is based an Orthogonal Transform, Malakooti Orthogonal Transform (MOT), as well as Malakooti-Saffari Scrambling Algorithm (MSSA) to apply multiple levels of security on the image files prior to delivery. The image scrambling and Encryption techniques are applied to provide the sufficient security and to reduce the risk of any attack during the delivery over the mobile networks. Our method can be divided into four steps as following: First, the image file is converted into RGB color space, and then the MSSA algorithm is applied on each layer of RGB, Red, Green, and Blue Matrices in order to scramble the image pixels and to provide the first level of security. In the second step, scrambled, R, G, B matrices are divided into smaller blocks and then MOT, Discrete Cosine Transform (DCT), or Walsh-Hadamard Transform (WHT) is applied on each sub-block to provide second level of security on the image. In the third step, we have generated sequences of secret keys (key) by using Malakooti Randomized Key Generator (MRKG) Algorithm and XOR operation is applied on the elements of the sub-block and the elements of the secret keys to provide third level of security on the image. Finally, the scrambled and encrypted sub-blocks of three layers, R, G, B matrices are combined together to build a highly secured scrambled and encrypted image ready to be transferred over the mobile networks.

Once the scrambled and encrypted image is transferred over the mobile networks, the reverse operation is applied to retrieve the original image. We applied our model on several different images and also calculated the MSE to show the efficiency and accuracy of our method over the existing ones. Since the mobile devices and wireless networks have a lot of limitations for the real time processing of the multimedia information, we have applied a fast orthogonal transform (MOT) and compared its result with DCT and WHT.

Index Terms: Encryption, Decryption, Scrambling, DCT, MOT, Orthogonal Transform, Mobile, Wireless, Security

1. INTRODUCTION

The major problem of any computer network is to prevent the access of important information from the illegal user or to hide and disclose the information from the intruders. One way to apply the security on the network information or to retrieve the secured information from the network is the Encryption/Decryption process [1].

In the last decades the digital communication networks, Wired and Wireless, have been developed rapidly and information can be transferred among networks easily. With the rapid advances in Internet Technology and embedded computing systems, the capturing of multimedia data (images, videos, audio) is being used more and more rapidly in applications such as video-on-demand, video conferencing, broadcasting and so on. To maintain the privacy or security, some sensitive information must be protected before the transmission or distribution [2].

In order to transmit secret images over the mobile network, a variety of encryption schemes have been developed. These schemes can be classified into three major types: position permutation [4], [5], value transformation [1]-[3] and visual transformation [6]. We have used the combination of the position permutation and value transformation by using our scrambling algorithm, MOT,DCT, or WHT transformation, along with the XOR operation of the secrete keys with the result of scrambled and processed image.

The conventional cryptographic mainly have been developed for the encryption of the alphanumeric data rather than the image and audio signals. The encryption and decryption of multimedia signals with traditional encryption systems required considerable amount of time for the computational process.

A fast, reliable, and robust algorithm is required to encrypt and decrypt both image and audio with less computation time and high degree of accuracy [7].

The challenges of multimedia such as digital images, documents, audio, and video come from two facts that multimedia data size is usually very large and need to be processed in the real time. To obtain a high secure transmission performance when applied to a high bit-rates multimedia data, it requires high processing resources and fast algorithm due to the complexity of computations used in the modern multimedia communications.

Discrete Cosine Transform, Hamard Transform, Malakooti Transform and other orthogonal transforms have been widely used in various signal-processing applications due to its fast and low cost inverse transform. We have proposed a fast digital scrambling algorithm along with a lossless encryption method based on the orthogonal transforms, DCT, WHT and MOT. Using the orthogonal transforms enable us to obtain the fast and high accuracy multimedia information during the decryption process.

2. MOBILE COMMUNICATION

2.1 MOBILE LIMITATION

There are many practical constraints in design and implementation of any software for the mobile multimedia which make this scheme not too practical. Some of these constraints are due to User Interface challenges when we switch from the desktop design to mobile application and the other can be considered as the platform problems; because there is not any unique platform that all mobile applications can be executed under that platform.

Smart mobile phones have opened up a new and exciting world of communication but also created its own problem and limitation due to various architecture and platforms. Thus we have to take into account the mobile device limitation and design the type of software that works properly and efficiently over the mobile networks while respecting unique constraints posed by each platform.

2.2 MOBILE SECURITY

The security applied on cellular data networks using GMS and GPRS technologies is weak and make it easy for the hacker to monitor the transmission of information among users by using an older GSM phone that has been partially reprogrammed. Although, the infrastructure for applying the security is designed to handle this problem but the government eavesdropping consideration and control and block of Voice over IP, VoIP is against such improvement [8]. This means that any improvement on the security for business application over Smartphone must be done by the end user. One way to apply additional security is to establish a Virtual Private Network (VPN) for mobile device user or apply an efficient and robust encryption algorithm before the transmission process.

3. RELATED WORKS

Encryption is the act of changing the content of the digital data, voice or image into a format that no one can recognize the detail of the encrypted file except those who have privilege to access the file and know the detail of some secret key(s) and decryption algorithm. Almost all devices that are connected to network are vulnerable to attack by intruder and all digital information should be encrypted to be secured and protected form the access of unauthorized ones. Mobile device also are accessing open network and their transmitted information are vulnerable to attack by hackers. Thus it is wised that all mobile information, especially transmitted ones, to be encrypted and protected from unauthorized watcher. Most of the available cryptographic algorithms are mainly designed for the encryption and decryption of large scale computers, servers, personal computer and laptops. Almost all existing encryption algorithms generates some type secret key that can be used to apply XOR operation of the image or processed image with the secret key. The key size is usually large for the larger devices and not very many encryption algorithms are developed with smaller keys for the smaller devices like cell phones, smart cards, and so on. Shanker, T.N. et al [9] has introduced an algorithm based on the Elliptic Curve Cryptography (ECC) for the image encryption of mobile devices. The ECC is an encryption algorithm for mobile devices that can be used to encrypt the image file before transmission. Martina Podesser, et al [10] has introduced an algorithm based on the Selective Bit Plane Encryption for Secure Transmission of Image Data in Mobile Environments. The Selective Bit Plane Image Encryption is the trade off between security and computational complexity because the real-time encryption for the entire video streams using classical cipher required much computational time. As the wireless networks have lots of limitation, it is necessarily to improve the communication between two points. Stefano Marano has presented a novel approach to deal with the non-line-of-sight (NOLS) propagation that relies solely on the features extracted from the received waveform. He has concentrated on the identification and mitigation for localization based on UWB experimental data [10]. Farruh Ishmanov has investigated a comprehensive overview that is related to energy consumption balancing in wireless networks [11].

4. Proposed Method

We have proposed a method that is based on the scrambling, linear transformation, and XOR operations with secret keys. Our multilevel security algorithm is lossless, reliable, fast, and robust because we have permuted all image pixels and then applied an orthogonal transforms along with XOR operation to increase the security of the encrypted image before transmission. The algorithm is easy to apply on all mobile devices for both transmission and receiver sides.

4.1 Design Goals

The main goal of encryption is to provide a high level security on all image files before the transmission process is applied as well as Provide a fast and reliable decryption process for all clients using the mobile networks. The proposed secure image delivery on Mobile Networks has been designed with the following objectives:

- **Security**: The confidentiality of data is ensured by using a robust ad strong Encryption/Decryption Algorithm. Image file is converted into RGB Color space and each color matrix R, G, B is divided into sub-blocks and the permutation process is applied on each sub-block to perform scramble process. The orthogonal transform is also applied on the scrambled sub-block and the XOR operation is applied on the result and the secret keys generated by MRKG Algorithm.
- **Strong Access Control**:
  We have applied three level of security on each image file based on three operations, Scrambling, Transformation, and XOR Operations to enhance the security of the image files and protect them against any unwarranted access.
- **Transparent Performance**:
  Encrypted/Decrypted files should behave similarly and have no differences from the file structure point of view.
- ***Convenience:***
  The system should be user friendly and convenient to use.

4.2 **Encryption Algorithm**

1- Load the image file from the mobile device

2- Convert the image file into RGB Color space

3- Divide the elements of RGB matrices into sub-blocks and

Apply Malakooti-Saffari Scrambling Algorithm on each sub block

4- Apply Malakooti Orthogonal Transform on each scrambled sub-Blocks of R.G.B matrices.

5- Generate Secret Keys by using Malakooti key Gen Algorithm

6- Apply the XOR operation on each scrambled, transformed

Sub blocks of R, G, and B matrices.

7- Combine three scrambled, transformed, XOR applied R, G, B

Matrices together and put them together as one image file.

8- Send the encrypted image into the final destination by using mobile network transmission.

Figure 1 illustrates the structure of encryption algorithm:

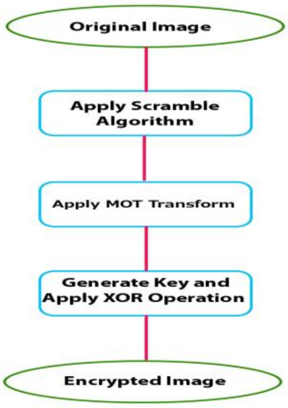


Figure 1-Encryption Algorithm

4.3 Malakooti-Saffari Scrambling/Descrambling Algorithms

We have applied Malakooti-Saffari Scrambling Algorithm to exchange the pixel location and divert its appearance. Our scrambling algorithm is applied to perform the first level of security on the image that is going to be delivered over the mobile networks. Figure 1 has shown the content of one block 0f 8 x 8 Red matrix from RGB color space.

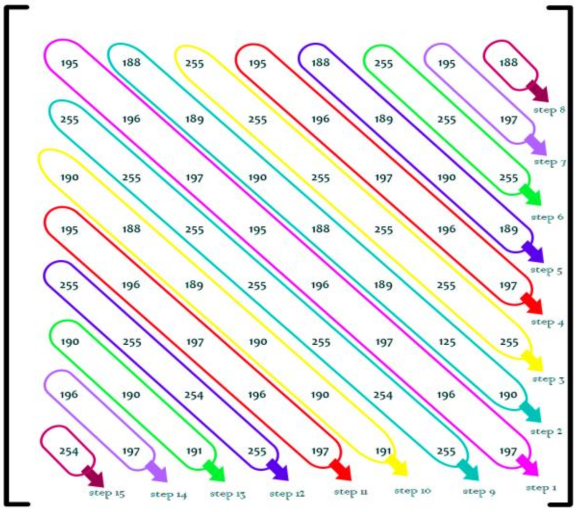


Figure 2- Graphical Representation of MSSA

As we have shown in Figure 2 the elements of the Main diagonal as well as elements of all upper and lower diagonals of the selected 8x8 blocks, ImgR, have been moved to one array, A, and the rows of new 8x8 scrambled matrices are formed using the array elements from the top to the bottom to create scramble matrix, ImgRSc, as following:

```
Step 1)   Index=0; Inc=1; M=N-Inc;(N is Block Size)
Step 2 )  for (I=0;I<N;I++) A[Index++]= ImgR [I][I];
Step 3)   While (M>=0) {
              for (I=0;I<M;I++) A[Index++]= ImgR [I][I+Inc];
              for (I=0;I<M;I++) A[Index++]= ImgR [I+Inc][I];
              Inc=Inc-1;M=N-Inc; }
 Step 4)  for (I=0;I<N;I++)
              for (J=0;J<N;J++)
                ImgRSc[I][J]=A[I*N+J];
```

Our Descrambling Algorithm is the reverse operation of the Scramble algorithm but it will be applied as last stage of the decryption process to retrieve the decrypted or original image.

4.4 Malakooti's Key Generator Algorithm

To apply the second level of the security we have used Malakooti Randomized Key Generator Algorithm to generate randomized secret keys required for XOR operation of scrambled image values with the secrete keys.

The Block Diagram MRKG Algorithm, Figure 3, as well as the pseudo code have shown the detail of the algorithm.

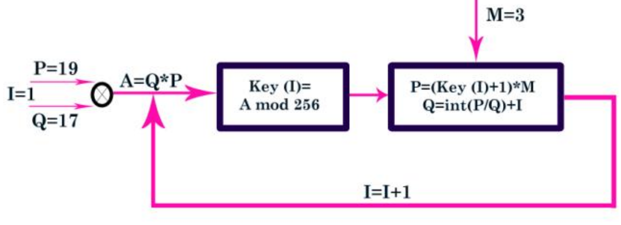


Figure 3- Block Diagram MRKG Algorithm

Inputs = P, Q, M (Prime Numbers)

Outputs = Array of Secret Keys

```
Step1) Enter three Prime Numbers for P, Q and M
          P = 19, Q = 17 and M =3
Step2) A= P*Q, i=1
Step3) Ki = A mod 256
          P  = (Ki+1)*M
          Q = Int(P/Q)+i
          A = P * Q, i=i+1
          if i<=N the go to step 3 , ( N is RGB block Size)
Step4) end
```

4.5 Apply Malakooti Orthogonal Transform (MOT):

A new Orthogonal Transform, Malakooti Orthogonal Transform (MOT), has been developed for the second stage of image encryption. The inverse of MOT like other orthogonal transform can be calculated as the ratio of the matrix transpose over some scalar number. Since the matrix transpose operation can be done through the index manipulation the time required for the inverse operation of the MOT depends upon the time of dividing all elements of the MOT into the scalar number. These properties make the MOT fast and very useful for the encryption/ decryption of images during the transmission over the Wireless Mobile Networks. The MOT algorithm is shown as following:

MOT Transformation:

```
For(I=0;I<N;I=I+2)
  For(J=0;J<N;J++)
      ImgScT[I,J]=ImgSc[I,J]+ImgSc[I+1,J];
For(I=0;I<=N;I=I+2)
  For(J=0;J<=N;J++)
      ImgScT[I,J]=-ImgSc[I,J]+ImgSc[I+1,J];
```

Inverse of MOT Transformation:

```
For(I=0;I<N;I=I+2)
  For(J=0;J<N;J++)
      ImgSc[I,J]=(ImgScT[I,J]-ImgScT[I+1,J])/2;
For(I=0;I<=N;I=I+2)
  For(J=0;J<=N;J++)
      ImgSc[I,J]=(ImgScT[I,J]+ImgScT[I+1,J])/2 ;
```

4.6: Comparison of MOT, DCT, WHT:

We have applied our algorithms on several images and compared the speed of operations with other orthogonal transform such as DCT and WHT. The required time for the entire operation such as Scrambling, XOR operation, and encryption have been measured and the result is shown in Table 1.

We already have mentioned that mobile network have lots of limitation and slow algorithm cannot be applied on these types of networks. Thus the MOT transform is an ideal transform for image scrambling and encryption as well as descrambling Table 1 illustrates the elapsed time in milliseconds for the Scrambling, XOR operations as well as the Encryption/ Decryption transform algorithms. We have divided the test image into blocks of 512x512, 128x128, 64x64, and 32x32 and compared the result with DCT and MHT. The result of simulation clearly indicated that our algorithm based on MOT used less operation time then WHT and DCT and can be as a fast algorithm for image encryption over wireless and mobile communications.

Table 1- Comparison of DCT, WHT, and MOT

Type of Transformation Algorithm ⬇	Required Execution Time for Each Transformation (ms) ⬇			
	512x 512 Block	128x128 Block	64x64 Block	32x32 Block
DCT	256	137	90	68
WHT	107	91	70	31
MOT	27	18	10	6

5. Decryption algorithm

1- Receive the encrypted image from the mobile network.

2- Convert the encrypted image into RGB color space.

3- Divide the elements of RGB matrices into sub-blocks.

4- Generate Secret Keys by using Malakooti's Key Gen.

5- Apply the XOR operation on each scrambled, transformed

Sub blocks of R, G, and B matrices.

6- Apply the Inverse of MOT on each scrambled, transformed

Sub-blocks of R,G, B matrices.

7- Apply the Inverse of Malakooti-Saffari descrambling algorithm

on each sub-blocks of R,G, and B matrices.

8- Combine three Descrambled, Decrypted R, G, B matrices and covert them into image file.

9- Display the decrypted image.

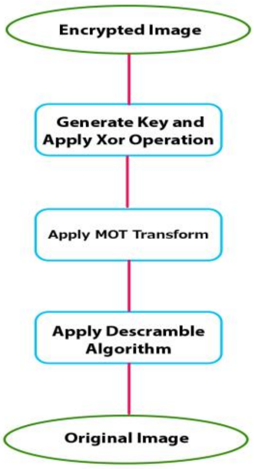

Encrypted Image
Generate Key and Apply Xor Operation
Apply MOT Transform
Apply Descramble Algorithm
Original Image

Figure 4- Illustrate Structure of Decryption Algorithm

6. Calculation of Minimum Square Error (MSE)

To test the accuracy of our algorithm we have calculated the Mean Square Error (MSE) of the original image and retrieved image after the descrambling and decryption processes are applied. MSE is the cumulative squared error between the original image and the recovered image and the smaller value of MSE indicates the closeness of the original image to the recovered image. MSE can be calculated from the following formula:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{J=1}^{N}(x_{ij} - x'_{ij})^2 \, (1)$$

Where x_{ij} and x'_{ij} are the pixel values of the original image and the recovered, descrambled, and decrypted, images.

Table 2- MSE of DCT, WHT, and MOT

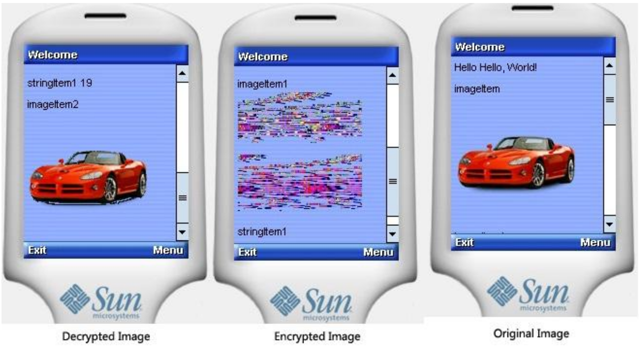
	512 x 512 Block	128x128 Block	64x64 Block	32x32 Block
DCT	8.367 E-9	6.249 E-9	5.640 E-9	5.079 E-9
WHT	7.84 E-15	4.75 E-15	0	0
MOT	6.95 E-17	5.74 E-17	0	0

The Mean Square Error of the encrypted images using DCT were almost close to zero, 5.079 E-9, when the size of the orthogonal transform matrices were 32 or less than 32 and we did not have a big even for block size of 64,128,256. The MSE of the encrypted images using both MOT and WHT were exactly zero for block size of 32 and 64 due to the structure of their transforms. The MSE for block size of 128 and 256 were almost close to zero and we can claim that we have lossless image encryption/decryption over mobile network. Figure 5 illustrated output of our proposed algorithm that we simulated it via mobile programming.

7. CONCLUSTION:

We have presented a new secure, fast and robust algorithm for the image delivery over the mobile network. Our proposed method is based on the new scrambling algorithm, Malakooti-Saffari Scrambling Algorithm, a new Orthogonal Transform. Malakooti Orthogonal Transform with the XOR operation of the secret keys generated by Malakooti key Gen Algorithm. Thus, we can claim that our algorithm has applied three levels of security on all images before the transmission over the mobile network. To prove the efficiency and fastness of our proposed method we have compared the result of encryption obtained by MOT as well as with the DCT and WHT. The empirical results obtained from Encryption supports our claim and Table -1 and 2 clearly has shown that MOT is faster than DCT and WHT. Clearly, our proposed method illustrates that our method has less cost rather than DCT and WHT, so it could be useful in mobile communications.

We also have suggested a new lossless compression algorithm to reduce the encryption time as well as to increase the operational Time.



8. REFERENCE

[1] Chang, C-C. "A New Encryption Algorithm for Image Cryptosystems", The Journal of Systems and Software 58, PP. 83-91,(2001).

[2] Pande, A. "Algorithms for Secure Multimedia Delivery over Mobile Devices and Mobile Agents", University of Washington, Seattle, WA, PP. 1-3, (19940.

[3] Sinha,A. Singh,K. "A Technique for Image Encryption Using Digital Signature", Optics com, PP. 1-6, (2003).

[4] Maniccam S.S, Bourbakis N,G. "Lossless Image Compression and Encryption Using SCAN", Pattern Recognition 34, PP. 1229-1245, (2001).

[5] Guo, J.-I, Yen, J.-C. "A New Mirror-like Image Encryption Algorithm and its VLSI Architecture", Department of Electronics Engineering, National Lien-Ho College of Technology and Commerce. PP. 4-7 (1999)

[6] Wu, X. Duncan, S. W, Qing, L. "Threshold Visual Cryptography Scheme for Color Image with No Pixel Expansion", ISCSCT 2009, Huangshan, China, 26-28 Dec 2009, PP. 310-315. (2009)

[7] Malakooti, M.V., Dobuneh, M.R.N., "A Lossless Digital Encryption System for Multimedia Using Orthogonal Transforms", DICTAP 2012, Bangkok, Thailand, May, PP. 240-244 ,(2012).

[8] Xenakis, C. "Security Measures and Weakness of GPRS Security Architecture", Internation Journal of Network Security, Vol. 6, No. 2, PP. 158-169, Mar. (2008).

[9] Shankar, T.N. , Sahoo, G. ; Niranjan, S. “Image Encryption for Mobile Device”, International Conference on Communication Control and Computing Technology, ICCCCT 2010, PP. 546-551. (2010).

[10] Stefano, M.“Survey of NLOS identification and error mitigation problems in UWB-based positioning algorithms for dense environments”, Springer Annals of Telecommunications, Vol. 65, No. 5, pp. 301-311, June 2010

[11] Ishmanov, F .“Energy Consumption Balancing (ECB) Issues and Mechanisms in Wireless Sensor Networks (WSNs): A comprehensive overview”, Wiley European Transactions on Telecommunications, DOI: 10.1002/ett.1466, Vol. 22, No. 4, pp. 151-167, 2011