ISSN No. 0976-5697

Volume 7, No. 2, March-April 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Digital Right Management Model Based on Cryptography for Mobile Multimedia Content

Pushpendra Verma
Research Scholar, Department of CSE,
Swami Vivekanand Subharti University, Meerut, U.P.,
INDIA

Dr. Jayant Shekhar
Professor, Swami Vivekanand Subharti University,
Meerut, Uttar Pradesh,
INDIA

Preety
Assistant Professor SIMC, Swami Vivekanand Subharti
University, Meerut, UP,
INDIA

Amit Asthana
Associate Professor, CSE, Department,
Swami Vivekanand Subharti University, Meerut, UP,
INDIA

Abstract: Cryptography is one field of science is the application of principles and mathematical methods to solve the problems concerning the security of information and data sent over the internet. By using the binary tree method, the digital image is converted into a secret password to keep your data safe. Step decrypt digital image by transforming the image into a binary matrix and then perform permutation KBRP who previously sequence of bits given action division bit per blok, after assembling bits into a binary tree and in the binary tree is given a key to turn it into a semi chipertexts, and finally recast the results of conversion bit into a matrix and then do a shift rows and columns so obtained chipertexts. Returns to the original image using the same symmetric algorithms. Based on the imagery used the result that there is some noise in the picture with an average of 40 dB, a good image quality and can be recognized as the original image.

The security required seems to be either compromised or not present at all besides, security costs money, resources and time and there is no one to pay for it either. The arena of Mobile Digital Rights Management consists of various players. End-user, Mobile Operator and Content Provider (and owner, publisher and retailer) being the legs of the tripod, the groundwork is to be laid by the technology providers of Infrastructure, Handset, Content Delivery Solution, Digital Rights Management Solution, Billing and Clearing.

Keywords: OMA- Open Mobile Alliance, DRM-Digital Right Management, CoIP : Communication over Internet Protocol, 3G-Third Generate

I. INTRODUCTION

In today‘s information age, data transmission plays an important role which is contributed to the growth of technologies. Electronic security is increasingly involved in making communications more prevalent. Therefore, a mechanism is needed to assure the security and privacy of information that is sent over the electronic communications media is in need. Whether the communications media is wired or wireless, both can’t be protected from unauthorized reception or interception of transmission. While modem cryptography is a vast and complicated field, the basics are easy to understand. In recent years, more and more businesses make use of communication networks, share potential information and therefore sensitive data is located in communications network transmissions that are connected all over the world. This commitment to data communication has increased the vulnerability of organization assets. Computer fraud is becoming one of the most popular crimes in our days.

Cryptography is necessary when communicating over any untrusted medium, which includes just about any particularly, the Internet. Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication: The process of proving one‘s identity
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original
- Non-repudiation: A mechanism to prove that the sender really sent this message

Digital Rights Management becomes important, which controls digital content usage under wireless environment. In a typical DRM model, a block cipher is usually used to encrypt multimedia content because of its reasonable security and performance. It is because users want long playtime and quick responsiveness with random access.

Multimedia content protection: While using the multimedia content through standby devices and through Internet, the end user wants a quick response for playing multimedia data. In general user feels uncomfortable if the response time exceeds one second. Playing the multimedia data after full decryption may not satisfy user’s requirement due to large size of data. So alternating with decrypting and playing data may be a good method to reduce sensory activation time.

Content protection by symmetric cipher: In cryptography symmetric and asymmetric cipher are used to prevent unauthorized access to multimedia content and illegal distribution. A symmetric key cipher uses the same key for data encryption and decryption and requires two communication parties share the key. The encryption

speed of symmetric key cipher is faster than that of asymmetric key cipher. A block cipher takes fixed-length groups of bits termed blocks from plain text as input and performs permutation and substitution (Schenier, 1996). Finally, same length of block is generated a cipher text. In CBC, encryption mode of block cipher encrypts each plaintext block with an adjacent cipher text block and key. Therefore, it can decrypt any specified block immediately with key because all blocks are cipher text.

The selective encryption: Multimedia data have different characteristics from text data. It is not necessary to encrypt data completely for protecting a huge multimedia file (Cheng and Li, 2000). In the area of multimedia security, "selective encryption" is devised to protect multimedia content and fulfill the security requirements for a particular multimedia application. Selective encryption is the technique of encrypting some parts of multimedia content while leaving others unencrypted. It may be a good alternative to full encryption since it can cause significant loss of quality during playing. Some multimedia applications such as TV broadcasting require much lower level security. In selective encryption, it is an important issue to determine which parts of data to be encrypted. Possible approaches are to encrypt some important parts of content; to divide content into fragments and then encrypt every Nth fragment; or to encrypt randomly chosen parts. Only encrypting some important part can show performance improvement. However, there are no general algorithms to select important parts of content. On the other hand, encrypting every Nth fragment of content is practically useless.

Related work: Many encryption algorithms are developed for securing images itself. By applying the principles of cryptography the images can be considered as data blocks or streams. Another method of image encryption is implementing scrambling algorithms for encrypting images by decomposing the original image into its binary bit planes. Zhou *et al*. (2009) proposed an image encryption algorithm by performing XOR operation with key image, inverting the components of bit planes and generate the encrypted image by selected scrambling method. Xiao and Xia (2008) proposed an image encryption algorithm in which the position of images are shuffled and states of hyper chaos are used to change the grey scale of the shuffled image. Amin *et al*. (2010) proposed an image encryption algorithm which encrypts 256 bits plain image to 256 bits cipher image using cryptographic primitive operations and non linear transformations.

Yoon and Kim (2010) proposed a new image encryption algorithm using a large pseudorandom Permutation which is combinatorially generated from small permutation matrices based on chaotic maps.

Tong and Cui (2008) proposed a new encrypting image scheme using the new compound chaotic function by choosing one of the two one-dimensional chaotic functions randomly. Zhi-Liang *et al*. (2011) proposed an image cryptosystem employing the Arnold cat map for bit-level permutation and the logistic map for diffusion. (Ali *et al*., 2007) proposed a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish.

Video encryption algorithms based on secret key and public key methods are formulated and public key cryptography is not applicable since the operations require large amount of time which is not suitable for video conferencing (Bojnordi *et al*., 2005). Video encryption algorithms can be classified as follows: Naive algorithm, selective algorithm, Zigzag algorithm, RC4 and AES. The idea of naive encryption is to encrypt video streams as byte by byte. Naive algorithm encrypts every byte in the whole video stream and these algorithms guarantee the most security level.

However, it is not an applicable solution if the size of the data is large. In selective algorithm, four levels of selective algorithms are suggested. These four levels are encrypting all headers, encrypting all headers and I (initial) frames, encrypting all I frames and all I blocks in P and B frames and finally encrypting all frames as in Naive algorithm to guarantee the highest security. The idea of ZIG-ZAG algorithm is basically encrypting the video streams before compressing them. Explicitly, when mapping the 8□8 block to a Ix64 vector each time in the same order. We can use a random permutation to map this transformation of the 8 x 8 block to the I x64 vector. Therefore, the concept of the encryption key does not exist in the ZIG-ZAG permutation algorithms. Once the permutation list is known, the algorithm will not be secure any longer.

Shi and Bhargava (1998) proposed a new video encryption algorithm called VEA depends on dividing the video streams into chunks. These chunks are separated into two different lists (odd and even lists).

Applying encryption algorithm like DES to the even list and the final cipher is concatenation of output of encryption algorithm XOR with the odd list streams. RC4 is stream cipher structure in which it encrypts plain text one byte at a time with variable length key size from 1to 256 bytes (8-2048). RC4 is a symmetric encryption algorithm in which the same key is used for encryption and decryption. The algorithm is based on the use of random permutation. RC4 is the most widely used stream cipher used in the SSL/TLS (Secure Socket Layer/Transport Layer Security) standards that have been defined for communication between web browsers and servers in which it encrypts plain text one byte at a time with variable length key size from 1-256 bytes.

II. PROPOSED ALGORITHMS

The objective of our research is both to protect and reduce the computational requirements compared to encrypting a whole file with only a block cipher and to strengthen security comparatively as that of selective encryption. A mechanism is needed to ensure the security and privacy of information transmitted via electronic communication media. Which requires a transmission to secure data sent over the internet? The method used is related to mathematics is the field of cryptography applications. As known to one very significant development is for the exchange of information or messages through the Internet. But that must be considered is the level of security of the information, because the Internet is an open network that is the Internet telecommunications infrastructure with open standards that can be used by many parties. Tapping the information is very harmful for the users of today's communications networks. With the wiretapping of communication of such information, the security aspects in the exchange of information are very important. This will make the communication network users feel safe and comfortable. In proposed algorithm the block of multimedia content is represented as binary tree in the initial step and matrix format in successive steps for row shifting and column shifting.

A. Protection uses a symmetric algorithm

In the prevention of unauthorized access to multimedia content and then used the illegal distribution of symmetric and asymmetric cryptographic cipher. Use the same key for encryption and decryption of data on the two sides share a key communication on the symmetric key. The required speed symmetric key cipher encryption much faster than asymmetric key cipher. A block cipher is taken from the same group bit length called a block of plain text as input and performs permutation and substitution. Thus, the same length as the resulting block ciphers text. All block cipher text is determined by key inferred from CBC saying that the block cipher encryption mode encrypts each plaintext block with an adjacent block cipher text and keys

B. Things are involved in the algorithm

There are several methods that are involved in the algorithm to be used, such as:

- Key-Based Randomized Initial Permutation (KBRP): beginning the process of randomization bit.

- Most Significant Bit and Least Significant Bit (MSB and LSB): used to assist in the formation of binary tree matrix.

- The binary tree traversal: trees, including one that is used for scrambling the bit and will generate pseudo chipertext.

- Shifting the matrix: used at the end of randomization, i.e. to obtain.

C. Key Based Random Permutation (KBRP)

Key Based Random Permutation (KBRP) is a permutation of certain key generated by considering all of these elements are given a key in the manufacturing process. In block cipher, used permutation to reset the message block. This permutation needs to be random and secret. Confidentiality of permutations depending on how produce them. Permutations are used in the block cipher as a mapping function that maps the elements of the message block in its original position to a new position. For example, the permutation P size 4 has four elements P [1], P [2], P [3], and P [4] the value is 3,4,1, and 2 respectively.

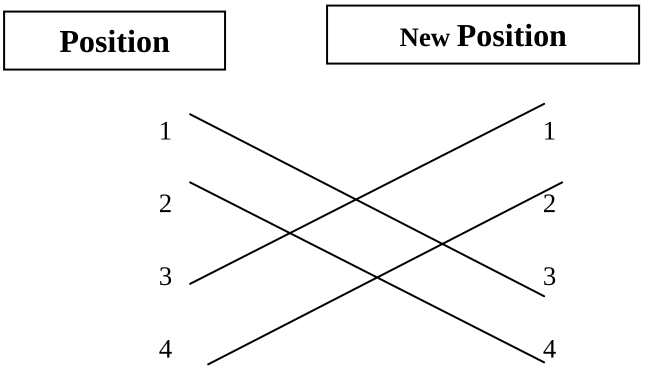


Figure1: Permutation KBRP

D. MSB and LSB

Least significant bit is part of a row of binary data (base two) which has the most significant value / smallest. Its location is a bit far right of the row. While the most significant bit is the opposite, namely the number of the most significant / most large and located next to the far left.

Example :

The binary number of 255 is 11111111 (sometimes given point b at the end of the numbers into 1111 1111b). These numbers may mean:

$(1 \text{ x } 2^7) + (1 \text{ x } 2^6) + (1 \text{ x } 2^5) + (1 \text{ x } 2^4) + (1 \text{ x } 2^3) + (1 \text{ x } 2^2) + (1 \text{ x } 2^1) + (1 \text{ x } 2^0) = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 225$

of line number 1 above, the rightmost number 1 is 1, and it is the smallest. This section is called the least significant bit (least significant bit), while the left-most valuable 128 and called the most significant bit (the most significant bit)

E. Graph Tree

The tree is a connected graph containing no circuit and has roots and leaves.

Some terms in the graph tree:

I. Node is an element tree that contains information / data and bookmark branching.

II. Level of a node is determined by first determining the root as multilevel 1. If a node is expressed as levels of N, the nodes that are children said to be in the level N + 1. There is also stated that the root is at level 0 and other nodes declared one storey higher.

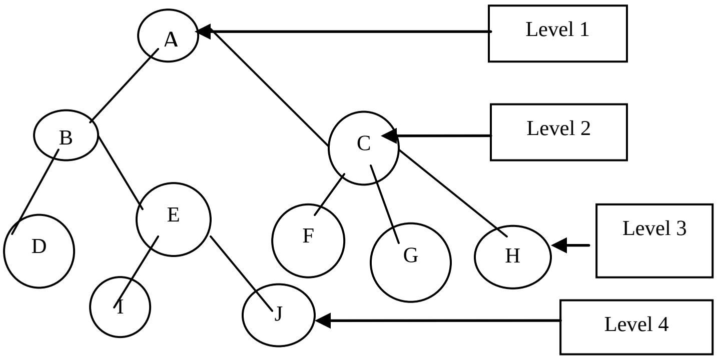


Figure 2. Structure of a tree

III. Degree (degree) of a vertex is expressed as the number of generations or a derivative of that node. Figure 2.4 node A has degree 2, B has degree 2, C has degree 3, E has a degree of 2. The nodes of degree 0 are called the leaf. Vertices D, I, J, F, G, H degree 0, called the leaves. The leaves are also often referred to as a node outside (external node), so the other node except the root is also often called a node (internal node).

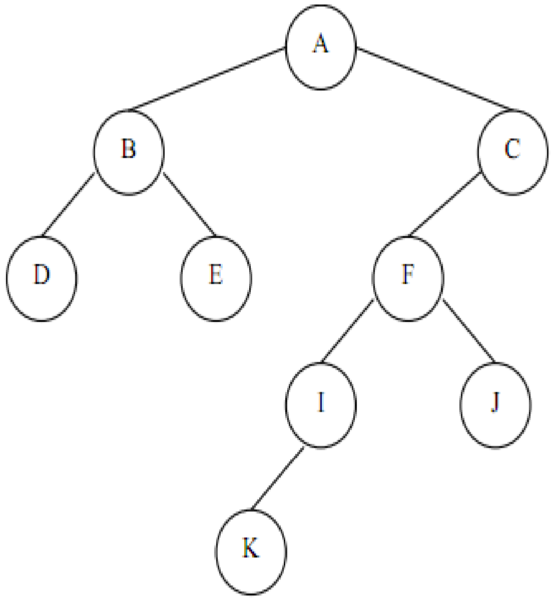
IV. Height (height) or depth (depth) of a tree is the maximum level of the nodes in the tree is reduced by 1. Tree Figure 1 has a depth of 3 or higher.

Binary tree (binary tree) may be defined as a collection of nodes that may be empty or have roots and are separated from each other subtree called the left sub-tree (left tree) and right sub-tree (right tree).

Binary tree characteristics, namely:

1. Each node has at most two children.
2. The highest degree of a node in a binary tree is two.
3. The maximum number of vertices at a rate of N = 2n-1.
Complete binary tree leaf level 3 has eight and the number of non-leaf node, including the root is 7.
Traversal order level that is visited node starting at level one to level node n.

Example : Reads A B C D E F G H I J K



Encryption algorithm:

The proposed algorithm of encryption the plaintext block by block and each block contains 2^{2n} bits. As the step first of the encryption process, each 2^{2n} bit plain-block is represented as a complete binary tree.

Step 1: Arrange the block of bits of size 2^{2n} as complete binary tree. The successive bits of the plaintext reside in each level and the construction of complete binary tree continues until for all bits of the plaintext. Suppose the plaintext f = B (l, x), l denotes each level of the binary tree and x would be the position of the node according to the permutation position, the MSB is at root node and the consecutive bits are added as left and right child at each level and the LSB is attached as leaf node and this node can be of left or right child of any node in the previous level of leaf nodes.

Step 2: A random permutation P is generated by key based permutation algorithm, so that P= {P1, P2, P3..Pn} is the subset of {1, 2…n}.

Step 3: assembling bits per block results permutation into binary tree traversal by making the MSB as the root and a row is added as a child of the left and right child then LSB is attached as a leaf node and this node can be a left child and right child at every level.

Step 4: Give the Z key to indicate the number of bits on all nodes, starting from the root node to traverse all levels to node x the number of all nodes sub tree rooted at x

$$Z = x + \sum_{\substack{k=all\ nodes\\ in\\ subtree\\ rooted\ at\ x}} (\mathbf{x},\mathbf{k}) \qquad \ldots\ldots\ldots\ldots.1$$

Step 5: If X = 0, the value of the node x is replaced by 0, if the value besides the node x is replaced with 1.

Step 6: Repeat the process for all nodes and the resulting bit is called cipher text pseudo (C1) where all nodes at position P1, P2, ……Pn.

Step 7: Set C1 into the matrix and assign the position that the roots were first in column and row first then arranged successively to column and the next line.

Step 8: Perform column wise downward shifting M times if the sum of permutation along column wise is even, otherwise perform column wise upward shifting M times. The resultant bits are termed as cipher text C

Decryption algorithm:

The cipher text C is given as input for the decryption:

Step 1: Reverse the permutation P as Pn, Pn-1…P1 and shifting rows and columns to restore the original position bits.

Step 2: set the bit into the binary tree traversal, the same way with encryption.

Step 3: Apply randomized substitution by choosing the node *x* at the position P_i of the binary tree

Step 4: enter key Z' to indicate the value of the bit. Eq. 2 denote the sum of bit values at all nodes, starting from root node, traversing all levels until the node x with the sum of all nodes of the sub tree rooted at x:

$$Z' = x + \sum_{\substack{k=all\ nodes\\ in\\ subtree\\ rooted\ at\ x}} \mathbf{x},\mathbf{k}) \qquad \ldots\ldots\ldots\ldots.2$$

Step 5: If Z'=0, the value at *x* is replaced by 0, otherwise the value at *x* is replaced by 1.

Step 6: The bits generated per block then apply the system of random permutations (KBRP).Repeat the process for all nodes at positions Pn, Pn-1Pn-2...P1 and the resultant bits are termed as pseudo plain text

Step 7: Stacking bits into the matrix

Step 8: Perform column wise upward shifting M times if the sum of permutation along column wise is even, otherwise perform column wise downward shifting M times. The plaintext bits are retained after decryption.

Personality Formation Algorithms:

The algorithm properly to decrypt the cipher text (C) into the original text .

A- Take a node x in a binary tree and let x Pi occupies a position in the substitution of the front. Let z equal to the sum of all values in all nodes begin x selected until all the nodes of a sub tree rooted at x .

- If z at node x is 0 then the fixed value 0 , if the value is more than 0 or other, then the value of the z change to 1 .

Properties of the proposed algorithm:

Correct algorithm to decrypt the cipher text (C) into the original text.

- Take a node x in a binary tree and let x Pi occupies a position in the substitution of the front. Let Z equal to the sum of all values in all nodes begin x chosen until all the nodes of a sub tree rooted at x.
- If Z at node x is 0 then a fixed value of 0, if the value is more than 0 or other than 0, then the value of the z transformed into one.

Property 1. The algorithm takes O (n), both for encryption and decryption.

Proof: The creation of binary tree takes O (n) time. The generation of pseudo random permutation takes O (1) time. Each substitution takes O(1) time. Since there are n elements to be replaced, substitution takes O (n) time and it is shown in Eq. 3:

$$\sum_{i=1}^{k}(1+2^{(k-1)} = \frac{k(k+1)}{2} + 2^{k}\left(1-\frac{1}{2^{k-1}}\right) = o_n$$

--------------3

Property 2: The algorithm correctly decrypts the cipher text C into the original plain text.

Proof: A node x in binary tree is taken and let x occupy the position Pi in forward substitution. Let z be equal to the sum of all values at all the nodes starting from the root node up to x plus the values at all nodes of the sub tree rooted at x.

Case 1: If z is even the value a = 0 at node *x*, if already a = 0 the result b = 0, since z-a is even number, if a = 1 at node x the result b = 0, z-a becomes odd. In decryption the value at b=0 at node *x* is retained as b = 0 = a, because z-b, z-a = even, if a = 1 then a is changed to b=0, because z-b = z-0 = (z-a)+a is even. Since (z-a) is odd, b is changed to a = 1.

Case 2: If z is odd, the value a=0 at node x is changed to b=1, therefore z= z-a = (z-1)+1 = (z-a)+a, if and only (z-a) is odd. In decryption the value b = 1 at node *x* is changed to a=0,therefore z = (z-a)+a = (z-a)+1=even,b=1 is changed to a = 0.If a = 1 then a is returned as b=1,z = (z-a)+a is odd,(z-a) is even, z = (z-a)+1 is odd, b = 1 is returned as a = 1.

III. RESULTS

The proposed algorithm is experimented for all types of multimedia files (images, music and videos).The multimedia content of any type is converted into binary format and applied to encrypt**ion. The encrypted image of flower** image by Blowfish algorithm and proposed algorithm is given in Fig. 1a-c. The results for music and video files show that the both encryption and decryption time for music and video files are lesser than their play time, so playing of both the files are started parallel along with decryption. The Table 1 and 2 show the experimental results of encryption and decryption time for image files, music files and video files. The results for music and video files show that the both encryption and decryption time for music and video files are lesser than their play time, so playing of both the files are started parallel along with decryption.

Table.1: Comparison of Encryption time of proposed algorithm with DES algorithm

File Type	File size	Encryption time	

		DES	Proposed algorithm
Image(.jpg)	4.3 MB	4.3 min	9.56 sec
Audio(mp3)	4.7 MB (play time:6 min) time:3 min)	18.48 min	1.56 min
Video(mp4)	255MB (play time:15 min)	45.37 min	7.13 min

IV. DISCUSSION

Security analysis: This section addresses the security of the proposed encryption technique and analysis of experimental results.

The pseudo random permutation which is generated by the key value has no influence on the plaintext recovered from the decryption process. It is because the key is only used to determine the pseudo random permutation and never used to change the value of any other bit in the plaintext.

Differential attack: To test the influence of one-pixel change on the whole encrpted image, two common measures NPCR and UACI are used. The Number of Pixels Change Rate (NPCR) measures the different pixel numbers between two images and UACI(Unified Average Changing Intensity) measures the average intensity of differences between the plain image and the cipherimage. For the calculation of NPCR and UACI, we have taken two encrypted images E_1 and E_2 and assume their corresponding plain images have only one-pixel difference

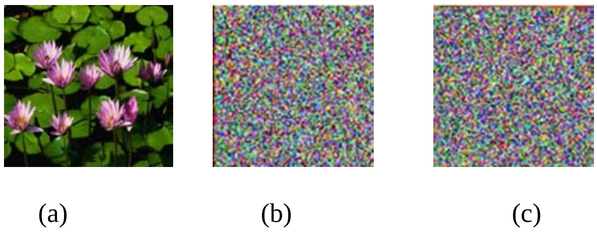


Figure 2: (a) Plain image), (b) Encrypted image by Blowfish algorithm, (c) Encrypted image by Proposed algorithm

Table 2: Comparison of decryption time of proposed algorithm with DES algorithm

File type	File size	Decryption time	
		……………………………………………	
		DES	Proposed algorithm
Image (.jpg)	4.3 MB	4.51 min	11.139 sec
	4.7 MB		
Audio (mp3)	(play time: 6 min)	4.8 min	9.98 sec
	76MB (play time: 3min)	25.48 min	2.43 min
Video(mp4)	255MB(play time:15 min)	52.37 min	11.28 min

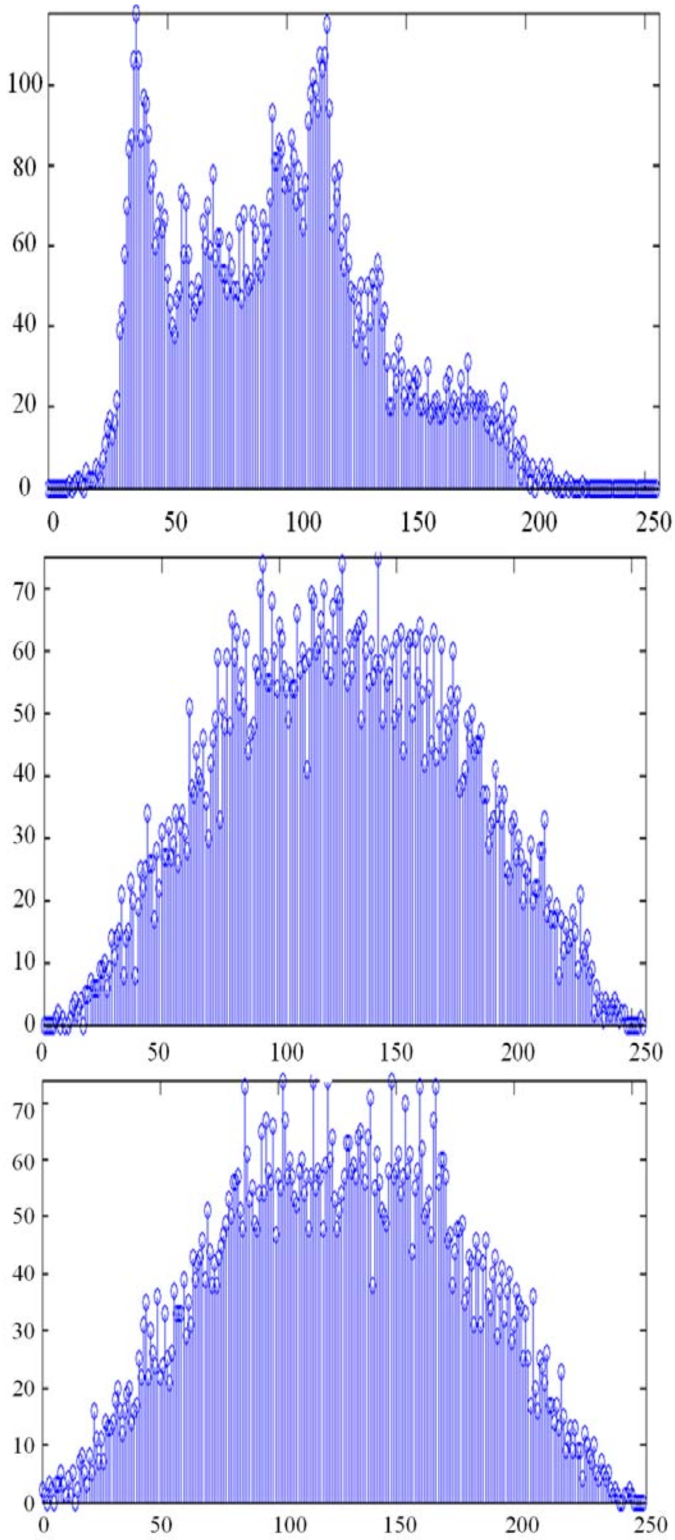


Fig. 2: (a) Histgram of Plain image,(b) Histogram Encrypted image by Blow fish algorithm,(c) Histogram of Encrypted image by proposed algorithm

Let W and H are the width and height of image and the gray-scale values of the pixels at grid (i,j) of E_1 and E_2 are labeled as $E_1(i,j)$ and $E_2(i,j)$ respectively. Define a bipolar array, D, with the same size as images E_1 and E_2. Then D(i,j) is related to $E_1(i,j)$ and $E_2(i,j)$, if $E_1(i,j) = E_2(i,j)$, then D(i,j) = 1 else D(i,j) = 0. The two measures NPCR and UACI are defined in Eq. 4 and 5 are given below

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W.H} * 100 \ldots\ldots\ldots\ldots\ldots\ldots\ldots 4$$

$$UACI = \frac{1}{W.H} * \frac{\sum_{i,j} |E1(i,j) - E2(i,j)|}{255} * 100 \ldots\ldots\ldots 5$$

Tests have been performed on the proposed algorithm, taking randomly a pixel of the original image and make a slight change on the gray-scale level of this pixel. The encryption algorithm is performed on the modified original image and the two measures NPC R and UACI are computed. We obtained NPCR = 99.85% and UACI = 33.58%. The results show that a slight change in the original image results in a great change in the encrypted image implies that the proposed algorithm has a good capability to resist the differential attack.

Histogram analysis: An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. The Fig. 2 gives the histogram of plain images and encrypted images. We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. The histogram of the cipher images from proposed algorithm are shown in Fig 2. The encrypted images bear no statistical resemblance to the plain image. It is clear that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.[5][6]

Correlation analysis: We have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image and cipher image, respectively. The procedure is done by randomly selecting 100 pairs of two adjacent pixels from an image. Then, the correlation coefficient is calculated using the following formulas in Eq. 6-9:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{Dx * \sqrt{Dy}}} \ldots\ldots\ldots 6$$

$$E(x) = \frac{1}{n} \sum_{i=1}^{n} X_i \ldots\ldots\ldots\ldots 7$$

$$D(x) = \frac{1}{n} \sum_{i=1}^{n} (x_i - \mathrm{E(x)}) * (x_i - E(x)) \ldots\ldots\ldots 8$$

$$cov(x,y) = \frac{1}{n} \sum_{i=1}^{n} (x_i - \mathrm{E(x)}) * (y_i - E(y)) \ldots\ldots\ldots 9$$

Correlation coefficients of randomly chosen 100 pairs of two adjacent pixels have calculated for plain image, cipher image encrypted by Blowfish algorithm and the cipher image by proposed algorithm. The correlation coefficients of plain image and encrypted images are given in Table 3.

	Plain	Encrypted image	Encrypted image
Direction	image	(Blowfish)	(proposed)
Horizontal	0.9816	0.0824	0.01776
Vertical	0.9858	0.0898	0.04912
Diagonal	0.9712	0.0548	0.00348

Table 3:Correlation coefficients of images

Cipher text only attack: In the cipher text-only attack, the attacker has to find the original values from the encrypted encryption the node value of the permutated position of the plaintext may or may not be changed related to the summation of node values along the path and the summation of the sub tree of the permutated position. Though the attacker is familiar with summation, based on that, he pseudo random permutation position Pi cannot be extracted since the replacement of bits are not performed for all substitutions.

Known plain text attack: In the known-plaintext attack, unauthorized user has both original plain text and the corresponding encrypted values. If we choose a sufficiently long plaintext sequence M1,M2,...,Mn and its corresponding cipher text C1C2…. Cn, look for a repetition in the cipher text, i.e., Cn1 = Cn2 for some integers n1 < 2,but the probabilities of occurring such cipher texts are low, so the attacker would not able to determine the pseudo random permutation sequence and also this sequence is mainly used for the bit position substitution.

Chosen plaintext attack: Suppose that the attacker has a privilege to execute the encryption machinery, he can choose plaintexts and generate their corresponding cipher text to recover the equivalent pseudo random permutation of bit positions to be traversed along the binary tree form of plaintext. Suppose the attacker chooses a plain text with all zeros as input to the encryption machinery and the cipher text would also be zeros not revealing the pseudo random permutation, which is used as key. From the cipher texts generated by chosen sequence of plain texts the number of 0`s and the number of 1's can be found out. But it is difficult to find out the order of 0's and 1's, since it amounts to checking for all n/2! Possible permutations.[5][6]

V. CONCLUSION

In this study, a new block cipher algorithm for multimedia cryptosystems is proposed. Based on the pseudo random permutation and substitution, using binary tree traversal, this values. According to our algorithm, for each cycle of the

proposed scheme encrypts any compressed multimedia content. While traditional algorithms and some existing chaotic schemes suffer from the poor diffusion operation, slow performance and small key space, our scheme has effective performance speed. The scheme is more secure for differential attacks, known plaintext attack, chosen plain text attack and able to encrypt large data sets with efficient and secure way. So, our algorithm is promising for real-time applications.

VI. REFERENCES

[1]. Ali, M., B. Younes and A. Jantan, 2007. Image encryption using block-based transformation algorithm. Int. J. Comput. Sci., 35: 1-9.

[2]. Amin, M., O.S. Faragallah and A.A.A. Et-Latif, 2010.A chaotic block cipher algorithm for image crypto systems. Commun. Nonl. Sci. Numer. Simulat., 15:3484-3497. DOI: 10.1016/j.cnsns.2009.12.025

[3]. Bojnordi, M.N., M.R. Hashemi and S.O. Fatemi, 2005. Implementing an efficient encryption block for MPEG video streams. Proceedings of 47th International Symposium, Jun. 8-10, IEEE Xplore Press, Zadar, pp: 127-130. DOI: 10.1109/ELMAR.2005.193659

[4]. Cheng, H. and X. Li, 2000. Partial encryption of compressed images and videos. IEEE Trans. Signal Proces.,48: 2349-2451. DOI: 10.1109/78.852023 Schenier, B., 1996. Applied Cryptography. 2nd Edn., John Wiley and Sons, New York.

[5]. Pushpendra Kr. Verma , Dr. J. Shekhar ,Preety and Amit Asthana" Digital right management to foster mobile multimedia services" in IJMIE ISSN No. 2249-0558, Vol. 2 Issue 4,pg 246-353, April 2012. http://www.ijmra.us.in

[6]. Pushpendra Kr. Verma , Dr. J. Shekhar ,Preety and Amit Asthana" Digital right management to foster mobile multimedia services" in ZENITH International Journal of Multidisciplinary Research ,ISSN 2231-5780 Vol.4 (1), pg 9-20 April 2012, JANUARY (2014). www.zenithresearch.org