An Efficient Image Digital Rights Management scheme with Multi Level Security

Sruthi K, Shiji S

Computer science and engineering Department, Nehru College of Engineering and Research Centre, Thrissur, India

Abstract - Technologies are fastly growing. Today image plays an important role in every one's life. Using cameras, scanners and other devices large number of image data are produced. These image data are convenient to spread and share via online network services and copy into offline storage devices. Misuse of confidential or commercial image data may lead to information security risk. Hence the protection of confidential image data is important. For this a confidential image data security (CIDS) scheme is introduced which is based on encryption, watermark, usage control and traceability. This scheme provides multi level security for an image while sending. Proposed Confidential image data security scheme have high security and efficiency.

Keywords: Digital rights management, Encryption, Watermark, Usage control, Traceability.

I. INTRODUCTION

Computer technologies are fastly growing. Due to this large number of images are produced from cameras, scanners and other devices such as mobile phones. Nowadays the usages of mobile phones are increased, so the productions of images are also increased multiple times. From these most of the images are shared through internet, some of them are confidential one, so its protection is important. Today large numbers of image protection mechanisms are used. Methods like encryption, watermarking etc. are used for protecting images. It is not visible to human visual systems.

Before sending an image it is to be encrypted for providing security. At the receiver end the same algorithm is used for decryption otherwise it may lead to the misuse of that image. In past decade to recent, most of the image security is mainly based on chaos encryption mechanism such as Arnold to protect the image. But its security is low and not so strong to resist attacks. It can provide security only in human visual system level. This current encryption mechanism doesn't provide usage control mechanisms such as control on image data usage times, backup or exports. If the image data was misused or leaked, there is no efficient way to find and trace the responsibility. To solve these problems a novel and efficient mechanism is needed.

For securing images now watermarking is used. Watermarking is mainly used for authentication purposes. After image authentication the watermark bits are extracted from it to detect the tampered area. For image content authentication many fragile or semi fragile watermarking method have been proposed. To detect the slight changes in the watermarked images fragile watermarking mechanism is used.

II. SYSTEM MODEL

The architecture of the confidential image data security (CIDS) scheme contain image encryption server, secure client user, secure exporting agent, and a misuse tracing agent. The architecture of the proposed CIDS scheme is shown in figure 2.1.

Images are produced in a plain mode. The usage control server decides the rights of that image. Usage control rights are the privileges given to the user of that particular image. Usage control rights are print, open, export and also set the number of times it can be open, print, and export. Usage control policy is set as the rights for that particular image. After encrypting the confidential image merge it with the rights to get the whole file.

After decrypting the image a legal user can only use these images under usage control policy. The usage control policy include image operations such as open times, print amount and export amount. Digital signature algorithm is used for providing integrity for this usage control policy.

The secure client user has the rights to export or transfer the confidential image data to an external user. But the export or transfer is strictly controlled by usage control policies. Before exporting, the confidential image data to be decrypted first and a watermark is embedded in to the confidential image. Sender's user identity and hardware related information is set as robust watermark. Before sending, the watermarked image is to be divided as grid and each grid is to be encrypted first. After encryption unsorted each grid and combine these grid to form an image and it is to be sending to the receiver side.

At receiver side, to get the confidential image the received image is to be divided first. For dividing images, same method is used at the sender and receiver side. After division sort the grids using reverse of the mechanism used in sender side. The sorted grids are decrypted and combine to get the confidential image. Once the exported

image is to be misused or leaked, the watermark is extracted from the exported confidential image and identifies the person who has the responsibility.

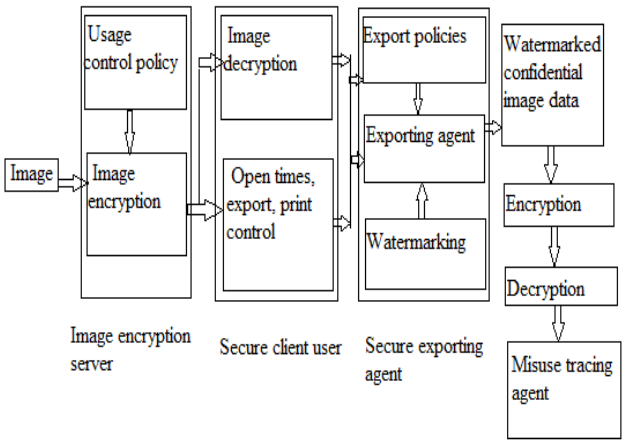

Fig. 2.1 Confidential image data security scheme

III. PREVIOUS WORK

The main image encryption scheme can be of three types that are partial selective encryption, visual cryptography, and full image content encryption. Image signal is distinctive in feature when compared with general signals that are strong correlation between adjacent pixels and great capacity of data. Partial encryption for digital images is based on spatial and frequency domains. In partial encryption select more sensitive parts that need more protection is encrypted using decoder or symmetric and asymmetric encryption. In visual cryptography, the image part to be protected is secretly shared and necessary parts of the separated images are combined together to recover the whole original image. For full content image encryption, the encryption mechanisms such as DES, 3 DES, AES etc. are used because of high processing speed of computer hardware.

Mainly watermarking is used for digital right management or authentication purposes with robustness or fragileness [1, 2]. This is suitable for identification and conformation of the original owner rights for digital images.

In Walton [3] introduced image tamper detection technique, for protecting gray scale image, first calculate the checksum of the seven most significant bit of the image and after that the calculated results are embedded in to the least significant bit of the randomly selected pixels. These methods effectively detect the tampered image. But these techniques have some drawback. First is an attack can exchange the pixels that will not affect the checksum of the image, these type of tampering will not be detected. Secondly, this scheme cannot indicate the tampered location of the tampered image. The third one is that the scheme cannot distinguish malice replacement and innocent adjustments. Lastly, for compressed images it is not an applicable technique. JPEG is a widely used compression standard for transmitting and storing digital images.

For image authentication purpose Wong [4] proposed a public key fragile watermarking scheme. In this the image is divided in to non-overlapping blocks and inserts a digital signature in to it. A key is used to generate a signature using the seven most significant bit of the pixel in each image block together with a logo which form a watermark and embed these watermark in to the least significant bit of the corresponding blocks. Wong and Memon [5] introduced an improved block wise authentication scheme, which uses an image index and a block index as the input to the hash function. But in this the verifier need to have prior knowledge about the image index, which is the limitation of this scheme.

IV. PROPOSED METHODOLOGY

A. Image Encryption

The image encryption server receives and replies to the confidential image encryption request. Using secure hash algorithm it create an image id for confidential image data that is to be used for encryption. After that the image encryption server defines the usage control rights for confidential image data. The defining rights are open times, print amount and export amount. The export right is provided for resending purposes. For providing security or integrity in usage control rights the image encryption server signs the rights using digital signature algorithm.

$$Sig = sign\ (Rights)$$

After creating confidential image data signature, the image encryption server encrypts the desired image using secret key.

$$C_{IID} = E_k(M)$$

After this, combines the cipher C and usage control rights and sig as a whole new cipher before sending.

B. Secure Client User

After encryption the combination of cipher text, rights, sig is sent to the client user. After deciphering the image, secure client can use this confidential image under control of usage control rights. After getting the cipher combinations read the sig and resign it. If the signature is valid then secure user can use this confidential image under these rights. Otherwise the user cannot open this image.

C. Secure Exporting Agent

If the client user needs to export the CIData (Confidential Image Data), the client user should check the exporting amount given in the rights. Exporting right is there then the secure client user embeds a watermark into it and the watermarked image is divided in to 9 parts. Each part of the grid is encrypted and unsorted. The unsorted parts are combined to form an image and that image is sends to desired one. On each export of CIData the export amount is decreased by 1 and verifies it before conducting another export.

1) Watermark embedding algorithm: Here first select the M × N binary image as watermark W. W=w(i, j); 0 ≤ i < M ,0 ≤ j <N and W(i, j) € {0,1}. Watermark is scrambled for providing more security and then scans the image in to 1D signal. ie, $W = \{w_i\},\ i = 1, 2, \cdots, C;\ C = M \times N, w_i = 0 \text{ or } 1.$ Select JPEG image as host image. The host image is divided in to 8 × 8 blocks. After zigzag the DCT coefficients, the whole sequence is recorded ie, *Di*(*j*), j = 0, 1, …..63., i is the sequence number of the block of the image. Select continuum of values to embed watermark, as

$$D_i(k-2), D_i(k-1), D_i(k), D_i(k+1), D_i(k+2)$$

Where k= 2, 3, ……..61;

2) AES Algorithm: Advanced Encryption Standard, also known as the Rijndael (pronounced as Rain Doll) algorithm is adopted worldwide. AES Algorithm is used to protect Electronic data. The first thing AES Algorithm needs is data and the other thing is key(encryption key).When these two combined are called as input and are feed into Cipher Engine produces Encrypted data in binary format called as cipher text. To recover the encrypted data it has to reverse the process in which the cipher text and key is feed into Cipher Engine to get back the original data. AES is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys. There are 10, 12, 14 rounds for 128,192 and 256 bit keys. Each round has certain processing involved. That are,
   a) SubBytes Transformation:-It uses substitution table which includes nonlinear substitution which operate on each byte of the state.
   b) ShiftRows Transformation:- In ShiftRows step, bytes in each row of the state are shifted cyclically to the left.The number of places each byte is shifted differs for each row. The first row doesn't change.
   c) MixColumnsTransformation:- MixColumns step operates on the column level. It is equivalent to the multiplication of matrix at column level. Each column of the state I multiplied with fixed polynomial.
   d) AddRoundKeyTransformation:- In Add RoundKey step, the state is combined with roundkey using XOR operation.

Expansion Key :- In AES algorithm, the sender and receiver is known about the key. The AES algorithm remains secure, the key cannot be determined any intruder even if he knows the plaintext and the cipher text. The larger the key the stronger is the encryption. The keys are then expanded using a key expansion routine for use in the AES cipher algorithm.

3) Watermark extracting algorithm: During the embedding process, obtain the same continuum of values for watermark extraction:

$$D_i(k-2), D_i(k-1), D_i(k), D_i(k+1), D_i(k+2)$$

Where k= 2, 3, ……..61;

Extracting method is,

$$\text{if } D_i(k) > \frac{1}{5}\sum_{l=k-2}^{k+2} D_i(l), \quad w_i = 1$$
$$\text{else} \quad w_i = 0$$

At last, anti-scramble the information to get the watermark extracted.

D. Misuse Tracing and Responsibility Confirmation

Once the watermarked CIData was misused, the Misuse Detecting Agent (MDA) in the CIDS (confidential image data security) scheme select the possible misused image and extract the hidden watermark. Using this extracted information MDA can trace the responsibilities of the confidential image data.

4) Tamper detection of CIDS scheme: Watermarked JPEG image is divided in to 8 × 8 blocks and apply DCT on each block. The tamper detection method is defined as follows:

$$\text{if } \mod(R(\frac{D_i(0)}{step}), 2) == 0, \quad \text{no } tamper$$
$$\text{else } tamper$$

$D_i(0)$ is DC coefficient in 8 × 8 block image, step is quantization steps, i=1, 2, ….., P × Q.

V. SIMULATION/EXPERIMENTAL RESULTS

The proposed CIDS scheme is not similar to traditional image encryption schemes. Firstly, CIDS encrypts full of the confidential image data content, which is the most important security attributes for confidential image data, and the security relies on the secure encryption algorithm. In CIDS scheme, used AES-CBC-256 algorithm as the encryption algorithm which is secure enough as data encryption standard.

In the full content image encryption experiments encrypted small size image files (under 10MB) and encrypted large size image files. Then calculated the average time elapsed, thus gained the encryption rate. Tables 1–3 gave detailed data of the full content encryption of variant size of images.

Based on the above groups experiments of variant amount image encryption, get high encryption efficiency and can satisfied the speed of real-time encryption even if the image size is over 30MB, and nearly all of the encryption rate reached near 40Mbps, which is very efficient and acceptable for full content encryption.

TABLE 1. FULL ENCRYPTION TIME IN VARIANT IMAGE DATA SIZE (SIZE<100KB)

Image	Size(KB)	Avg.time	Rate(Mbps)
Baboon.jpg	83.9	2.05	39.96
Barbara.jpg	85.42	2.11	39.53
Flowers.jpg	44.51	1.09	39.87
Fruits.jpg	40.17	0.98	40.02
Lenna.jpg	45.32	1.11	39.87
AVG	-	-	39.85

TABLE 2. FULL ENCRYPTION TIME IN VARIANT IMAGE DATA SIZE(3MB<SIZE<6MB)

Image	Size(MB)	Avg.time	Rate(Mbps)
1.jpg	3.18	80	39.75
2.jpg	3.26	82	39.53
3.jpg	3.17	79	40.12
4.jpg	4.71	118	39.91
5.jpg	4.23	106	39.9
AVG			39.84

TABLE 3. FULL ENCRYPTION TIME IN VARIANT IMAGE DATA SIZE(SIZE ABOVE 30MB)

Image	Size(MB)	Avg.time	Rate(Mbps)
1.jpg	31.12	779	39.94
2.jpg	32.52	814	39.96
3.jpg	33.97	850	39.96
4.jpg	30.4	761	39.94
5.jpg	32.37	809	40.01
AVG	-	-	39.962

The simulation results are evaluated successfully. The watermark contains information about the sender user id, computer id, mac id, or cpu id and, then can trace the responsibility of Confidential image data. The simulation results give watermarked image, division of watermarked image, encryption of image parts. Similarly on the receiver side the division of image, decryption of image parts and after combining gets the confidential image.

The simulation result shows that embedding of watermark inside the cover image is done effectively. The watermarked image is not distinguishable from original cover image. In these paper multi layer security is provided using watermarking, image division and AES encryption. Simulation results are shown below. Fig 5.1 shows the original image and watermark. Fig 5.2 shows watermarked image and division of watermarked image. Fig 5.3 shows the encrypted image parts.

Fig 5.1 a) Original image b) Watermark

Fig 5.2 c) Watermarked image d) Divide watermarked image

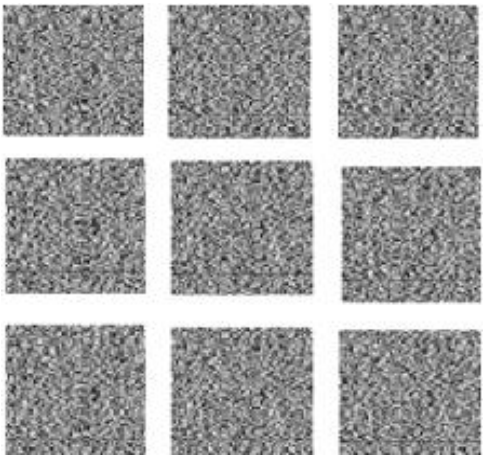

Fig 5.3 e) encrypted image parts

VI. CONCLUSION

This paper proposed a technique for image security using encryption, watermarking, usage control and traceability. The original image is encrypted first and usage control

rights are merged in to it as signature before sending it to the authenticated person. The usage control right gives the exporting rights for the authenticated person. At the time of exporting watermark is embedded into host image. After that the watermarked image is to be divided and encrypt each image parts and combining these parts after unsorted the encrypted parts. The reverse of this is applied at the receiver side. In proposed Confidential Image Data Security scheme multi level security is used while sending an image. So this scheme is highly secure and efficient.

VII. FUTURE SCOPES

While sending an image security is the important thing to be considered. In this research work multi level security is provided for an image on sending. Providing more security to this scheme a onetime password security mechanism is taken as future work.

REFERENCES

[1]. J. Park and R. Sandhu, "UCON ABC usage control model", *ACM Transactions on Information &System Security*, Vol.7, pp.128–174, 2002.

[2]. P.W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification", *IEEE Transactions on Image Processing*, Vol.10,No.10, pp.1593–601, 2001.

[3]. S. Walton, "Image authentication for a slippery new age", *Dr. Dobbe's Journal*, Vol.20, No.9, pp.35–42, 1995.

[4]. P.W. Wong, "A public key watermark for image verification and authentication", *Proceedings of IEEE international conference on image processing*, pp.455–463, 1998.

[5]. M.Y. Syue and L.J. Wang, "A Wavelet-based multipurpose watermarking for image authentication and recovery", *International Journal of Communications*, Vol.2, No.4, pp.35–39, 2013.

[6]. Uhl and A. Pommer, *Image and Video Encryption*, *Springer Press*, pp.45–134, 2005.

[7]. Lini Abraham and Neenu Daniel, "Secure image encryption algorithms: A review", *International Journal of Science &technology*, Vol.2, No.4, pp.186–189, 2013.

[8]. N.K. Pareek, V. Patidar and K.K. Sud, "Image encryption using chaotic logistic map", *Image and Vision Computing*, Vol.24, No.9, pp.926–934, 2006.

[9]. A. K. Osama and A. M. Zin, "An efficient adaptive of transparent spatial digital image encryption", *Procedia Technology*, Vol.11, No.1, pp.288–297, 2013.

[10]. K. Ramani, E.V. Prasad, S. Varadarajan, *et al*., "A robust watermarking scheme for information hiding", *International Conference on Advanced Computing and Communications*, pp.58–64, 2008.

[11]. D.M. Ferdinando and S. Salvatore, "Fragile watermarking tamper detection with images compressed by fuzzy transform", *InformationSciences*, Vol.195, No.13, pp.62–90, 2012.

[12]. S. Rawat and B. Raman, "A chaotic system based fragile watermarking scheme for image tamper detection", *AEU- International Journal of Electronics and Communications*, Vol.62, No.10, pp.840–847, 2011.