Verification of Authenticity of Transmitted Images

Kh. Manglem Singh

DOEACC Centre, Imphal – 795001, Manipur, India
Telephone: 0091 385 2454109, 2452231, Fax: 0091 385 2449578
E-mail: manglem@gmail.com

Abstract

This paper proposes a new technique for the verification of authenticity of transmitted images through the Internet. The scheme works on the combination of the chaotic cat map for the scrambling the addresses of the pixels, the Hamming code for the encryption of pixel values and the digital signature for the verification of tampering. The digital signature of the original image is added to the encoded version of the original image to be transmitted. At the receiver end, comparison is performed between the embedded digital signature from the received image and computed digital signature from the received image to verify the authenticity of the image.

1. Introduction

Today all networks are connected to the global Internet. More and more information has been transmitted over the Internet. Information is in many forms – text, audio, image and other multimedia. The image has been widely used in our daily life and is an important data class. It may be the diagram of army emplacements, diagram of bank building construction and the important data captured by military satellite. Nowadays, high-resolution pictures are freely available on the Internet and are provided by many sites in addition to Google Earth. Indian security agencies are still upset that high-resolution images of Indian military bases and government buildings are visible on Google Earth (http://geocarta). Indian authorities are concerned that state-of-the-art Sukhoi 30 MKI fighter planes were caught on camera. However, images of sensitive US installations, such as the White House, have been blurred out from Google Earth. Images are used for the identification of people, verification of cards and other identities. The media content must be protected in applications such as pay-per-view TV, confidential video conferencing, medical imaging, in medical and military imaging systems. Reliable image encryption techniques are of utmost importance for the protection of data from counterfeiting, tampering, unauthorized access and fraud. And the number of computer crimes has increased recently and many of them are related to images and videos. Image security has become an important topic in the current computer world.

Encryption of the image and audio data using the conventional methods of cryptography has certain limitations in the cryptographic strength and large computational effort due to huge amount of data and high correlation among pixels. Some of the popular public key encryption methods, such as RSA or El Gamal are not suitable for encryption of large data files and images, because their encryption rate is slow.
Moreover, the security of such public key cryptographic schemes relies on the inability to perform factorization of large numbers or to solve the discrete logarithm problem in a fast, efficient manner. However, the newly emerged field of quantum computing could, theoretically, make such methods totally unusable in the future (Fridrich).

It was mentioned in (Fridrich) to encrypt large data files with private-key symmetric block encryption schemes. Advances in cryptanalytic techniques and quantum computing threaten symmetric encryption schemes. Private key encryption algorithms, such as DES, 2DES, 3DES etc. are based on several iterative steps consisting of substitution and permutation. The security is mostly guaranteed by substitution, while the permutation part is somewhat neglected. It is general belief that utilization of complicated permutations might significantly increase the security of the whole cipher.

Chaos-based image-encryption approaches have shown some exceptional properties in the aspects concerning security, complexity, speed, computing power and computational overhead etc (Fridrich, Chen et al. 2004). Many researchers have proposed different types of such encryption. Kuo proposed an encryption method that obtains the encrypted image by adding the phase spectra of the plaintext with those of another key image (Kuo 1993). The cipherimage is unrecognizable, since the phase spectra of the original image are randomly changed. Chang and Liou (Chang et al 1994) proposed an encryption method that first compresses the image by using a quadtree and then encrypts the compressed data by SCAN language. Chang and et al. used vector quantization for image encryption (Chang et al 2001). Image encryption technique using the XOR operation (Han et al 1999) was proposed. This method is very simple, but is weak to the chosen/known-plaintext attack.

Yen and Guo proposed an encryption method, known as BRIE based on the chaotic logistic map (Yen et al 1999). The basic principle of BRIE is bit recirculation of pixels, which is controlled by a chaotic pseudo random binary sequence. In the chaotic key-based algorithm, a binary sequence of keys is generated using a chaotic system (Yen et al 2000). The image pixels are rearranged according to the generated binary sequence and then XORed and XNORed with the selected key. This method is weak to the chosen/known-plaintext attack using only one plain image (Li et al 2002). Scharinger proposed the chaotic Kolmogorov flow based image encryption (Scharinger 1992). The whole image is taken as a single block in this scheme, and which is permuted through a key-controlled chaotic system based on the Kolmogorov flow. In order to confuse the data, substitution is applied, which alters the statistical property of the cipher-image. The scheme is computationally secure and superior to contemporary block encryption systems for the image and video data encryption. For advancing the quality of encryption effectively, the method of position scrambling can be used before encryption. Some classical scrambling algorithms are the cat map (Chen et al 2004, Chung et al 1994, Fridrich 1997, Fridrich 1998), baker map (Fridrich, Mao et al 2004), affine transformation (Chang 2004), magic-square transformation (Arthur et al 2001), knight-tour transformation (Charilaos et al 2000), standard map, tent map etc. Among these maps, the cat map, standard map and baker map attract much attention. The cat map is a two-dimensional chaotic map introduced by Arnold and Avez. The baker map is another two-dimensional chaotic map based on which Pichler and Scharinger first introduced their encryption schemes. In (Fridrich) a symmetric image encryption scheme based on 3-D chaotic cat map was proposed. The 2-D chaotic cat map was generalized to 3-D for
designing a real-time secure symmetric encryption scheme, which employed 3-D cat map to shuffle the positions of image pixels and used another chaotic map to confuse the relationship between the cipher-image and the plain-image. In (Matthews 1989), the baker map was further extended to 3-D. An alternative chaotic image encryption based on the baker map that supports a variable-size image and includes other functions such as password binding and pixel shifting to further strengthen the security of the cipher-image was proposed (Jakimoski et al 2001).

In (Baptista 1998), Baptista proposed a chaotic encryption based on partitioning the visiting interval of chaotic orbits of the logistic map. Li and et al. proposed chaotic video encryption scheme (CVES) that generates pseudo random signal to mask the video and to perform pseudo random permutation of the masked video (Li et al 2002).

Haist and Tiziani (Haist et al. 1998) proposed a method that recognizes counterfeit objects based on the digital signature. Sinha and Kehar (Sinha et al 2003) proposed an image encryption technique for secure image transmission using the digital signature that encrypts the image by adding it, bit-wise, to the encoded version of the original image. In their technique, image encoding is done using Bose-Chaudhuri Hocquenghem (BCH) code. Encinas and Dominguez (Encinas et al 2006) commented to (Sinha et al 2003) that the secret key and the original image can be recovered efficiently by a brute force attack.

We propose a new technique for the verification of authenticity of transmitted images through the Internet. Comparison between the embedded digital signature from the received image and computed digital signature from the received image verifies the authenticity of the image.

The rest of this paper is organized as follows. Section 2 discusses the main features of the chaotic cat map, Hamming code and digital signature. Section 3 describes the proposed technique. Section 4 is on the experimental results. Finally, Section 5 concludes the paper.

2. Base Theory
2.1 Cat Map

The classical Arnold cat map is a two-dimensional chaotic map (http://mathworld) described by

\[
\begin{bmatrix}
  x_{n+1} \\
  y_{n+1}
\end{bmatrix} = \begin{bmatrix}
  1 & a \\
  b & ab + 1
\end{bmatrix} \begin{bmatrix}
  x_n \\
  y_n
\end{bmatrix} \mod (N)
\]

(1)

where \((x_n, y_n)\) is the pixel position in the \(N \times N\) image and \(x_n, y_n \in \{0, 1, 2, 3, ..., N-1\}\); \((x_{n+1}, y_{n+1})\) is the transformed position after the cat map; \(a\) and \(b\) are two control parameters and are positive integers.

The cat map preserves area, since the determinant of its linear transformation matrix is equal to 1. It is one-to-one mapping, that is, each point in the matrix can be transformed to another point uniquely. Image position is scrambled via the iteration of the cat map, consequently realizing the image encryption. The result of scrambling is different for difference of the iteration times. Periodicity changes for different parameters of \(a\) and \(b\) and the size of the image. The two parameters \(a\) and \(b\) are the key of the cat map.

2.2 Hamming Code

A Hamming code is a linear error-correcting code named after its inventor, Richard Hamming (http://en.wikipedia.).
Hamming codes can detect and correct single-bit errors, and can detect (but not correct) double-bit errors. Figure 1 shows the 8-bit data, denoted by $D_1D_2D_3D_4D_5D_6D_7D_8$ and its corresponding 12-bit Hamming code, by $P_1P_2D_1P_3D_2D_3D_4P_4D_5D_6D_7D_8$. $P_i$ ($i = 1$, 2, 3 and 4) denotes the parity bit.

8-bit data

\[
\begin{array}{cccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
D & D & D & D & D & D & D & D \\
\end{array}
\]

(a)

Hamming code

\[
\begin{array}{cccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
P_1 & P_2 & D_1 & P_3 & D_2 & D_3 & D_4 & P_4 \\
9 & 10 & 11 & 12 \\
D_5 & D_6 & D_7 & D_8 \\
\end{array}
\]

(b)

Figure 1.
(a) 8-bit data  and
(b) Corresponding 12-bit Hamming code.

The algorithm of the Hamming code for an 8-bit pixel value is as follows:

1. All bit positions that are powers of two are used as parity bits. (positions 1, 2, 4 and 8).

2. All other bit positions are for the data to be encoded. (positions 3, 5, 6, 7, 9, 10, 11, and 12).

3. Each parity bit calculates the parity for some of the bits in the code word. The position of the parity bit determines the sequence of bits that it alternately checks and skips.

- Position 1: check 1 bit, skip 1 bit, check 1 bit, skip 1 bit, etc. (1, 3, 5, 7, 9 and 11).
- Position 2: check 2 bits, skip 2 bits, check 2 bits, skip 2 bits, etc. (2, 3, 6, 7, 10 and 11).
- Position 4: check 4 bits, skip 4 bits, check 4 bits, skip 4 bits, etc. (4, 5, 6, 7 and 12).
- Position 8: check 8 bits, skip 8 bits, check 8 bits, skip 8 bits, etc. (8, 9, 10, 11 and 12).

4. Set a parity bit to 1 if the total number of ones in the positions it checks is odd. Otherwise, set it to 0.

Table 1 gives the parity bits of the Hamming code and their corresponding data bits.

<table>
<thead>
<tr>
<th>Parity bit</th>
<th>Corresponding data bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1$</td>
<td>$D_3$, $D_5$, $D_7$, $D_9$, $D_{11}$</td>
</tr>
<tr>
<td>$P_2$</td>
<td>$D_3$, $D_6$, $D_7$, $D_{10}$, $D_{11}$</td>
</tr>
<tr>
<td>$P_3$</td>
<td>$D_5$, $D_6$, $D_7$, $D_{10}$, $D_{12}$</td>
</tr>
<tr>
<td>$P_4$</td>
<td>$D_9$, $D_{10}$, $D_{11}$, $D_{12}$</td>
</tr>
</tbody>
</table>

2.3 Digital Signature

The digital signature is created by a one-way hash function. A hash function is used, because it is unique for a particular message and is difficult to revert. The digital signature is logically associated with a message. Message authentication is concerned with protecting the integrity of a message, validating identity of originator and non-repudiation of origin (dispute resolution). There are many standard algorithms that convert a message of any length into a fixed length message digest,
usually 128, 160, 256, 512 bit long. MD5, SHA1, RIPEND, HMAC (Stallings 2001) etc. are some standard techniques for a hash.

3. Proposed Technique

The block diagram of the proposed technique is shown in Figure 2. The original image is used for computing the digital signature by MD5, SHA1 or RIPEND. Scrambling of addresses of pixel values of the image is then performed by using the chaotic cat map. The image is then encoded using an appropriate Hamming code. The digital signature is added bitwise in the pixel of the encoded image. The encoding and bit insertion result the encrypted image. This addition is done only in any one of the positions in the data bits, and not in the parity bits of the Hamming code. This ensures that the bits of the digital signature can be extracted from the Hamming code correctly. The size of the pixel values of the encrypted image increases due to the added redundancy by the error control coding. The digital signature is treated like additive noise that can be recovered at the receiver end after transmission.

The decryption of the encrypted image is shown in Figure 2(b). The digital signature is recovered bitwise from the encrypted message. The decoder can detect one-bit error that has been corrupted by the digital signature. The Hamming decoder corrects the error. The chaotic cat map is then applied to the decoded message for reassembly the addresses of the scrambled pixels. The digital signature is computed from the recovered image using the MD5, SHA1 or RIPEND. The recovered signature and the extracted signature are compared for authenticity of the image.

![Figure 2 (a) Block diagram of the encryption procedure and (b) Block diagram of the decryption procedure.](image_url)

3.1 Hamming Code Encoder

The parity bit of the Hamming code encoder for 8-bit data is computed as follows:

\[
P_i = \begin{cases} 
D_1 \oplus D_2 \oplus D_4 \oplus D_5 \oplus D_7 \\
D_1 \oplus D_3 \oplus D_4 \oplus D_6 \oplus D_7 \\
D_2 \oplus D_3 \oplus D_4 \oplus D_8 \\
D_5 \oplus D_6 \oplus D_7 \oplus D_8 
\end{cases} \quad (2)
\]

where \(i = 1, 2, 3, 4\).

3.2 Hamming Code Decoder

The parity bit is again computed by using Equation (2) at the receiving end from the received data to check whether the transmitted data and received data are identical. Error-bits are found as follows:

\[
e_i = P_i \oplus PD_i \quad (3)
\]
where $P_i$ and $PD_j$ are the parity bits generated at the transmission and receiving ends respectively for $i = 1, 2, 3, 4$.

$e_i$ can be either 0 or 1 depending on whether the same data is received at the receiving end or not. Table 2 gives the list of probable erroneous bits and corresponding $e_i$ combinations.

<table>
<thead>
<tr>
<th>Erroneous bits</th>
<th>Error-bit combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_1$</td>
<td>$e_1, e_2$</td>
</tr>
<tr>
<td>$D_2$</td>
<td>$e_1, e_3$</td>
</tr>
<tr>
<td>$D_3$</td>
<td>$e_2, e_3$</td>
</tr>
<tr>
<td>$D_4$</td>
<td>$e_1, e_2, e_3$</td>
</tr>
<tr>
<td>$D_5$</td>
<td>$e_1, e_4$</td>
</tr>
<tr>
<td>$D_6$</td>
<td>$e_2, e_4$</td>
</tr>
<tr>
<td>$D_7$</td>
<td>$e_1, e_2, e_4$</td>
</tr>
<tr>
<td>$D_8$</td>
<td>$e_3, e_4$</td>
</tr>
</tbody>
</table>

Table 2: List of probable erroneous bits and corresponding error-bit combinations

The correct data-bit at the receiving end is computed as follows:

$$CD_j = \begin{cases} (e_1, e_2, e_3, e_4) \oplus D_1 \\ (e_1, e_2, e_3, e_4) \oplus D_2 \\ (e_1, e_2, e_3, e_4) \oplus D_3 \\ (e_1, e_2, e_3, e_4) \oplus D_4 \\ (e_1, e_2, e_3, e_4) \oplus D_5 \\ (e_1, e_2, e_3, e_4) \oplus D_6 \\ (e_1, e_2, e_3, e_4) \oplus D_7 \\ (e_1, e_2, e_3, e_4) \oplus D_8 \end{cases}$$

where $j = 1, 2, ..., 8$.

4. Experimental Results

Simulation was performed by using MATLAB software on a Pentium IV PC to verify the validity of the proposed encryption technique. 8-bit grayscale images of the Lena, Mandrill, Miramar, Kodak, House and Hut of $256 \times 256$ size were used in the experimentation. The message digests of the images generated by using the MD5 were given in Table 3. Hamming (12,8) error control code was used to encode the original image before the addition of the digital signature. Results were taken in Equation (1) of the chaotic map for the control parameters having values of $a = 1$, $b = 1$ and $N = 256$. The periodicity of the cat map for these parameters is 383.

The digital signature of the original image was added to the encoded image in a way that it causes a single bit error in the data bit of the Hamming code. Figure 3 shows the original Lena image, along with scrambled image after applying the cat map, result of the cat map and Hamming code together and recovered image. By flipping a single bit in Figure 3(d) resulted a tampered image. The digital signature of the tampered Lena image obtained by flipping the least significant bit (LSB) of the encrypted image at $(10,16)$ address location is dfb75933f35ffce8f0255d9f323aa6d23, which is different from the original signature 8a23d5f547c952427b182af10c8a3e30. The digital signature was recovered at the receiving end after the Hamming decoder was applied. The digital signature of the recovered image was extracted from the recovered image after the Hamming decoder and cat map were done. The authenticity of the transmitted was verified by comparing the two digital signatures.

The size of the pixels for the encrypted image is 12. Table 4 show the first 16 raw pixel values of the original Lena image and their corresponding encrypted values after applying the cat map, Hamming encoder and insertion of the digital signature. Figure 4 shows another set of results on the original Miramar image.
5. Conclusions

This paper proposed a technique that uses an encryption scheme for the image based on the combination of the chaotic cat map for the scrambling the addresses of the pixels, the Hamming code for the encryption of pixel values and the digital signature for the verification of tampering of the transmitted image. The size of pixels increases due to the added redundancy. The comparison of the recovered digital signature from the encrypted image and the computed digital signature using the recovered image verifies the authenticity of the transmitted image.

Figure 3  (a) Original Lena image, (b) Result of the cat map (c) Result of the cat map and Hamming code and (d) Recovered image.
Figure 4 (a) Original Miramar image, (b) Result of the cat map (c) Result of the cat map and Hamming code and (d) Recovered image.

Table 3: Images and their message digests

<table>
<thead>
<tr>
<th>Image</th>
<th>Message digest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>8a23d5f547c952427b182af10c8a3e30</td>
</tr>
<tr>
<td>Mandrill</td>
<td>5524a4c037be76b1287656718aa7b5ef</td>
</tr>
<tr>
<td>Miramar</td>
<td>9e99822064fb36579751d3377de1c1d7</td>
</tr>
<tr>
<td>Kodak</td>
<td>86d825b3c86bd142476fffe295222e7</td>
</tr>
<tr>
<td>House</td>
<td>ebd4858c1eafca5e4ef2cee3bf30576c</td>
</tr>
<tr>
<td>Hut</td>
<td>fe82b13d7e25619bc48e5a3dfd9e0d9</td>
</tr>
</tbody>
</table>

Table 4: Pixel values of the original Lena image and corresponding encrypted image

<table>
<thead>
<tr>
<th>Raw pixel values</th>
<th>Encrypted pixel values</th>
</tr>
</thead>
<tbody>
<tr>
<td>162 161 156</td>
<td>1874 443 1214</td>
</tr>
<tr>
<td>160 160 159</td>
<td>2144 2641 421</td>
</tr>
<tr>
<td>162 154 155</td>
<td>2260 239 3535</td>
</tr>
<tr>
<td>160 156 157</td>
<td>856 1629 2910</td>
</tr>
<tr>
<td>157 151 154</td>
<td>1629 830 2854</td>
</tr>
<tr>
<td>155</td>
<td>2821</td>
</tr>
</tbody>
</table>

References


http://mathworld.wolfram.com/arnoldsCatMap.html
