A Semi-Fragile Image Content Authentication Technique based on Secure Hash in Frequency Domain

P. D. Sheba Kezia Malarchelvi
(Corresponding author: P. D. Sheba Kezia Malarchelvi)

Professor, Department of Computer Science and Engineering, J.J. College of Engineering and Technology
Ammapettai, Tiruchirapalli-620009, Tamil Nadu, India.
(Email: pdsheba@yahoo.co.in)

(Received June 20, 2011; revised and accepted August 28, 2011)

Abstract

Image Authentication techniques enable the recipients to verify the integrity of the received image. In this paper, a semi-fragile image authentication technique based on secure hash generated with Orthogonal Polynomials based Transformation (OPT) coefficients is proposed. In this proposed scheme, the content based image feature is extracted from the OPT domain and the image hash which is used to verify the originality of the image is generated using the extracted features. In order to make the proposed scheme robust to content preserving image processing manipulations, the inter-coefficient relationship among OPT coefficients is exploited. Experimental results indicate that the proposed scheme is semi-fragile that is, the scheme is tolerant to unintentional manipulations like lossy compression and additive noise while being sensitive to malicious attacks like replace and crop.

Keywords: *Image content authentication, integrity, orthogonal polynomials, inter-coefficient relationship*

1 Introduction

The increasing need for trustworthy distribution of digital multimedia in business, industry, defense etc. has lead to the concept of content-based authentication. Nowadays manipulating digital images efficiently and seamlessly has become very easy with the availability of powerful software and hence, it is necessary to ensure confidentiality as well as integrity of the images that are transmitted. Image encryption schemes [7, 9, 15, 16] are used to ensure confidentiality while content authentication mechanisms check the integrity of the image received, by ensuring that the image sent by the sender has not undergone malicious manipulations. The focus of this paper is on devising a novel image content authentication technique.

MD5, SHA-1 and other traditional cryptographic content authentication methods [10, 16] are not suitable for visual data since they are extremely sensitive to the message; i.e., changing even one bit of the input message will change the output dramatically. However, multimedia data such as digital images undergo various manipulations like compression and enhancement while transmission. These processes change the pixel values of the digital image but not its content and so they should not affect the authenticity of the data. image content authentication requires techniques which should be resilient to content preserving manipulations like lossy compression, while at the same time be fragile enough to detect malicious manipulations.

Image content authentication schemes can be broadly classified into two types: watermark-based and hash-based signature systems. Watermarking based techniques embed an imperceptible signal into a cover to form a watermarked image. At the receiver, the extracted watermark from the watermarked image is used for authentication purpose. A survey of different watermarking schemes used for image content authentication is presented in [7]. In [23] P.W. Wong *et al.* have proposed a public key watermark system that generates the watermark by calculating exclusive-or of a bi-level watermark image and a hash value is obtained using MD5 from the original image. The signal is digitally signed by the private key of the public key cryptosystem and is embedded in the least significant bits of the pixels of the original image. The verification system extracts the embedded signal, and verifies it using the public key. Then it calculates the hash value from the candidate image and recovers the bi-level watermark image by calculating exclusive-or of the embedded signal and the hash value. In [25], Shensheng Yu *et al.* have proposed an authentication system in which content based watermark is generated from the LL3 component of three-level Haar wavelet decomposition using Sobel edge detection and then the hash is computed using MD5 as the hash function. The computed hash is then embedded in the middle frequency coefficients. Fridrich and Goljan [5] proposed a method for self-embedding an image as a method of protecting the image content. This method also allows the regions of the image that have been tampered with, cropped, or replaced, to be partially repaired. The basic principle of this method is to embed a compressed version of the image into the LSB of its pixels. The major drawback of this method is that embedded information is not robust.

In contrast to the watermark-based techniques, hash based techniques extract a set of features from the image to form a compact representation that can be used for authentication. One of the advantages of hash-based techniques is that no distortion is introduced in the image that is to be authenticated. Several hash based signature systems have been reported in the literature. These systems use data from different domains such as pixels [5, 17], DCT coefficients [4, 6, 11, 12, 18, 19, 21, 24], Wavelet transform coefficients [1, 2, 13, 22] and Fourier transform coefficients [5], to the generate signature. Schneider *et al.* have proposed a digital signature system in [17] for image authentication, that uses the intensity histogram to calculate the feature vector over which a hash is computed and public key encryption algorithm to sign the generated hash. The Euclidean distance between the hash computed at the receiver and the hash received from the sender is compared against a chosen threshold to determine the degree of modification that is acceptable. C. Lin and S. F. Chang [12] have proposed an image authentication technique that relies on the invariant relationship between any two selected DCT coefficients which are at the same position of two different (8 x 8) image blocks. Their scheme is sensitive to catch malicious manipulations made in a part of an image and at the same time is resilient to JPEG compression. In [24], Xie *et al.* have suggested the use of Approximate Message Authentication Codes (AMAC) for image authentication. The AMAC is a probabilistic checksum computed by applying a series of XOR operations and two rounds of majority bit voting in DCT domain. The similarity between two images is determined using the hamming distance of their AMACs. In [11] Lin et al. have used the property that the relationship between a pair of DCT coefficients of the same coordinate position in two different blocks remains the same before and after JPEG compression because all DCT coefficient blocks are divided by the same quantization table, for authentication of images as well as video. The feature codes of the image records the relationship of the difference value. If the difference is greater than or equal to zero a 1-bit is recorded otherwise a 0-bit is recorded. The authentication procedure checks whether the same relationship holds at the receiver. They have also suggested the use of multilayer feature codes to protect the DCT difference values within more precise ranges. In [6] Fridrich and Goljan have proposed the generation of 50-bits for every (64 x 64) DCT block by projecting the blocks on to a set of 50 orthogonal random patterns with the same size (64 x 64), generated by a secret key. The final hash value of the image is obtained by concatenating the hash codes from all the blocks. Takeyuki Uehara *et al.* have proposed a JPEG-tolerant image authentication system with adjustable security in [21]. This system constructs a Message Authentication Code (MAC) incorporating a number of feature codes that are used to protect regions of interest in the image. The system is designed to tolerate JPEG compression and does not tolerate other types of acceptable manipulations. In [19] Q. Sun and S. F. Chang have proposed a semi-fragile image authentication solution combining Error Correction Codes (ECC) and watermarking. By using ECC, they provide a mechanism that allows minor variation of content features caused by acceptable manipulations such as lossy compression and additive noise. I-Chuan Chang *et al.* have proposed two image authentication schemes in [4], one based on error detection codes and the other based on HMAC. In [13], Chun-Shien Lu *et al.* have proposed a geometric distortion resilient image hashing scheme for copy detection and authentication with a mesh generation algorithm in the lower-frequency component of an image in wavelet domain. A mesh normalization process is used to transfer the decomposed meshes of fixed sizes and a DCT based hash extraction method is employed to create a short binary hash sequence. Though the scheme is resilient to geometric distortion, it is very complex.

The scheme proposed by Fawad Ahmed *et al.* in [1], calculates the hash over LL2 DWT coefficients after permuting the pixels using a permutation key. Bhattacharjee and Kutter have proposed an image authentication system that uses feature extraction, in [2]. This system transforms an image into wavelet coefficients using the Mexican Hat wavelets and constructs a set of feature points using a feature detection function. The verification system inputs a candidate image and calculates the set of feature points. The calculated set of feature points is compared against the received set of feature points. If the absolute difference between the two is less than 2, the input image is considered to be authentic. Venkatesan *et al.* [22] have proposed a robust image hashing scheme using wavelet transform wherein the extracted image hash is tolerant to acceptable manipulations like JPEG compression, low pass filtering, etc. and is different for different images. But this scheme compares the image as a whole and cannot localize tampered area in an image. In [3], Ee-Chien Chang *et al.* have described a content-based authentication scheme which is based on a weighting function that exploits the fact that important content information is not uniformly distributed across the image and that illegal operations are usually localized while permissible operations are global in nature. Through the use of scale-space salient points and wavelet foveation the scheme extracts a space-variant content-based signature for the image. In [20] Ashwin Swaminathan *et al.* have developed an algorithm for generating an image hash, based on Fourier-Mellin transform features which are invariant to two-dimensional affine transformations. The scheme also incorporates key-dependent randomization into the Fourier-Mellin transform outputs to form a secure and robust image hash.

Since image hashing schemes do not introduce distortions in the original image like the authentication schemes based watermarking, hash based authentication schemes, especially schemes that generate the content hash in the frequency domain are preferred for many applications due to their robustness. Hence in this paper, a frequency domain authentication technique based on the orthogonal polynomials based integer transformation is proposed. The proposed system exploits the inter-coefficient relationship between OPT coefficients at the same positions in pairs of transformed blocks and the system is designed to be tolerant to non-malicious distortions like lossy compression and additive noise.

The paper is organized as follows. In Sections 2 and 3, the proposed orthogonal polynomials based transformation is described. Section 4 elaborates the proposed authentication scheme and in Section 5 the experimental results are presented.

2 Orthogonal Polynomials Based Transformation

The Discrete Cosine Transform and Discrete Wavelet Transform are the most widely used transforms for image authentication. However the computational complexity of these transforms is quite high as they involve floating point operations. Motivated by the fact that integer transforms lower the computational complexity, the orthogonal polynomials based transformation which has proved to be efficient in image compression [8] has been used in the proposed image authentication scheme.

A linear 2-D image formation system is considered around a Cartesian coordinate separable, blurring, point spread operator in which the image *I* results in the superposition of the point source of impulse weighted by the value of the object *f*. Expressing the object function *f* in terms of derivatives of the image function I relative to its Cartesian coordinates is very useful for analyzing the image. The point spread function *M*(*x*, *y*) can be considered to be real valued function defined for (*x, y*) ∈ *X* x *Y*, where *X* and *Y* are ordered subsets of real values. In case of gray-level image of size (*n***n*) where *X* (rows) consists of a finite set, which for convenience can be labeled as {0, 1, …, *n*-1}, the function *M*(*x*, *y*) reduces to a sequence of functions.

$$M\,(\,i,\,t) = u_i(t),\; i,\,t = 0,\,1,\,\ldots,\,n\text{-}1 \tag{1}$$

The linear two dimensional transformation can be defined by the point spread operator *M*(*x*, *y*)(*M*(*i*, *t*) = *u*$u_i(t)$) as shown in Equation (2).

$$\beta'(\zeta,\eta) = \int_{x\in X}\int_{y\in Y} M(\zeta,x)\; M(\eta,y)\; I(x,y)\; dxdy \tag{2}$$

Considering both X and Y to be a finite set of values {0, 1, 2 … *n* –1}, Equation (2) can be written in matrix notation as follows

$$\left|\beta'_{ij}\right| = \left(|M| \otimes |M|\right)^t |I| \tag{3}$$

where ⊗ is the outer product, $|\beta'_{ij}|$ are n^2 matrices arranged in the dictionary sequence, |*I*| is the image, $|\beta'_{ij}|$ are the coefficients of transformation and |M| is

$$|M| = \begin{vmatrix} u_0(t_1)\,u_1(t_1)\cdots u_{n-1}(t_1) \\ u_0(t_2)\,u_1(t_2)\cdots u_{n-1}(t_2) \\ \vdots \\ u_0(t_n)\,u_1(t_n)\cdots u_{n-1}(t_n) \end{vmatrix} \tag{4}$$

We consider the set of orthogonal polynomials $u_0(t)$, $u_1(t)$, …, $u_{n-1}(t)$ of degrees 0, 1, 2, …, *n*-1, respectively to construct the polynomial operators of different sizes from Equation (4) for $n \geq 2$ and $t_i = i$. The generating formula for the polynomials is as follows.

$$u_{i+1}\,(t) = (t - \mu)\; u_i(t) - b_i(n)\; u_{i-1}(t) \text{ for } i \geq 1,\;\; u_1(t) = t - \mu, \text{ and } u_0(t) = 1 \tag{5}$$

where $b_i(n) = \dfrac{\langle u_i, u_i\rangle}{\langle u_{i-1}, u_{i-1}\rangle} = \dfrac{\sum_{t=1}^{n} u_i^2(t)}{\sum_{t=1}^{n} u_{i-1}^2(t)}$

and $\mu = \dfrac{1}{n}\sum_{t=1}^{n} t = \dfrac{n+1}{2}$

Considering the range of values of t to be $t_i = i$, $i = 1, 2, 3, \ldots n$, we get

$$b_i(n) = \frac{i^2\left(n^2 - i^2\right)}{4\left(4i^2 - 1\right)} \tag{6}$$

As shown in Equation (4), we construct the orthogonal polynomials operator |*M*| based on the orthogonal polynomials in Equation (5). |*M*| can easily be made an integer transform by scaling its elements appropriately.

3 The Orthogonal Polynomial Basis

For the sake of computational simplicity, the finite Cartesian coordinate set *X*, *Y* is labeled as {1, 2, 3}. The point spread operator in Equation (3) that defines the linear orthogonal transformation for image coding can be obtained as |*M*| ⊗ |*M*|, where |*M*| can be computed and scaled from Equation (4) as follows.

$$|M| = \begin{vmatrix} u_0(x_0) & u_1(x_0) & u_2(x_0) \\ u_0(x_1) & u_1(x_1) & u_2(x_1) \\ u_0(x_2) & u_1(x_2) & u_2(x_2) \end{vmatrix} = \begin{vmatrix} 1 & -1 & 1 \\ 1 & 0 & -2 \\ 1 & 1 & 1 \end{vmatrix} \tag{7}$$

The set of polynomial operators O_{ij}^n $(0 \leq i, j \leq n\text{-}1)$ can be computed as $O_{ij}^n = \hat{u}_i \otimes \hat{u}_j^t$ where $\hat{u}_i$ is the $(i+1)^{st}$ column vector of |*M*|. For example polynomial basis operators of size (2 * 2) are

$$\left[O_{00}^2\right] = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \left[O_{01}^2\right] = \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix},$$

$$\left[O_{10}^2\right] = \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix}, \left[O_{11}^2\right] = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

Polynomial basis operators of (3 * 3) are

$$\left[O^3_{00}\right]=\begin{bmatrix}1&1&1\\1&1&1\\1&1&1\end{bmatrix},\quad \left[O^3_{01}\right]=\begin{bmatrix}-1&0&1\\-1&0&1\\-1&0&1\end{bmatrix},\quad \left[O^3_{02}\right]=\begin{bmatrix}1&-2&1\\1&-2&1\\1&-2&1\end{bmatrix}$$

$$\left[O^3_{10}\right]=\begin{bmatrix}-1&-1&-1\\0&0&0\\1&1&1\end{bmatrix},\left[O^3_{11}\right]=\begin{bmatrix}1&0&-1\\0&0&0\\-1&0&1\end{bmatrix},\left[O^3_{12}\right]=\begin{bmatrix}-1&2&-1\\0&0&0\\1&-2&1\end{bmatrix}$$

$$\left[O^3_{20}\right]=\begin{bmatrix}1&1&1\\-2&-2&-2\\1&0&1\end{bmatrix},\left[O^3_{21}\right]=\begin{bmatrix}-1&0&1\\2&0&-2\\-1&0&1\end{bmatrix},\left[O^3_{22}\right]=\begin{bmatrix}1&-2&1\\-2&4&-2\\1&-2&1\end{bmatrix}$$

Having described the orthogonal polynomials based transformation, we propose an authentication scheme built upon these transformed coefficients, in the following section.

4. Proposed Authentication Scheme

In this section an image authentication scheme that can be used to verify the content integrity of gray scale images is proposed. This scheme is similar to the DCT based authentication scheme proposed in [12]. The proposed scheme is based on the invariant relationship between the OPT coefficients at the same positions in pairs of blocks chosen according to a mapping table constructed using the random sequence generated with the secret key. The technique is designed to be sensitive to intentional manipulations which affect the meaning of the image.

In this system, the hash generation process is incorporated into the quantization phase of lossy compression process by exploiting the fact that the relationship between the OPT coefficients in the same position of different sub-blocks of the image remains the same before and after quantization, since the same quantization matrix is used for all the sub-blocks during compression. Due to this, the system is tolerant to an optimal level of lossy compression. At the same time, the proposed system is capable of detecting and localizing intentional tampering of the image that may be caused by hackers.

The loss incurred during quantization, is due to the round off operation performed after scaling the transformed coefficients by the quantization value. But the difference between the coefficients belonging to same frequency position of different sub-blocks of the image remains the same before and after quantization. So of this property is exploited to generate a hash to verify the authenticity of the image since such a hash will tolerate a little loss.

In this proposed system, the image is first partitioned into non-overlapping blocks of size (N x N). The proposed orthogonal polynomials based transformation is then applied to get the OPT coefficients of each block [β'_{ij}] where $0 \le i < N$; $0 \le j < N$ and the coefficients are arranged in a 1-D zig-zag sequence [β'_k] where $0 \le k < N^2$. Two sub-keys k_1 and k_2 are generated from the secret key. The sub-key k_1 is used to generate a random sequence using which (n-1) β'_k s where (n-1) < N^2, are chosen from the first half of the zig-zag sequence and the feature vectors are formed using β'_0 and the chosen β'_ks. This ensures that the low frequency coefficients in which most energy is compacted due to the proposed unitary transformation, contribute to the feature vectors. Then a mapping table T whose entries are the random numbers generated using the sub key k_2 is constructed and employed to select the feature vector pairs whose coefficients are used to generate the hash code. The difference between the coefficients in the feature vector pairs P and Q is used to generate the hash bits 'h' as follows.

$$h=\begin{cases}1 & if\ ((P_{ij}-Q_{ij})\ge\tau)\\ 0 & otherwise\end{cases} \tag{8}$$

where $0 \le i < b/2$ and j = 0 to 3, b is the number of blocks (feature vectors) and τ is the tolerance value introduced in order to prevent the system from reporting some false alarms due to minor acceptable manipulations.

The image is then compressed by performing scalar quantization using a quantization factor CQ, entropy coded and then sent to the receiver along with the hash. The same process of selecting the coefficient pairs employed at the sender is used at the receiver to choose the coefficient pairs and the relationship between them is found to generate the hash bits. The hash produced at receiver is then compared with the received hash. The image is declared to be authentic if both the hashes are equal otherwise it is declared to be unauthentic. If the image is unauthentic, the blocks where a mismatch occurs are identified as tampered blocks and indicated.

The steps involved in this proposed hash generation with the OPT domain at the sender and receiver are presented diagrammatically in Figures 1and 2.

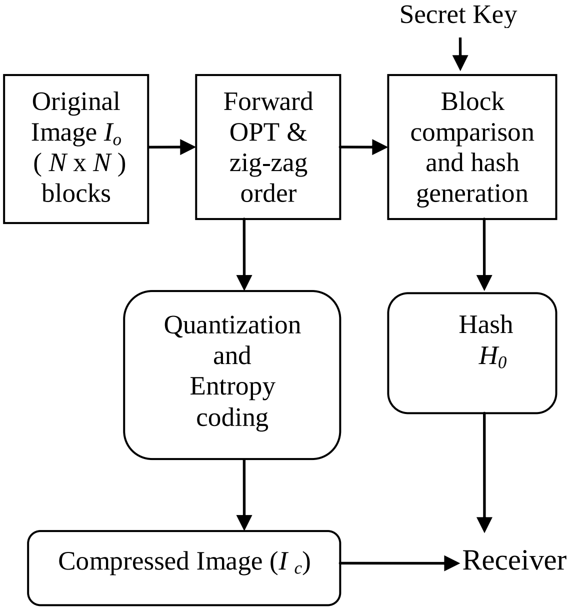

Secret Key
Original Image I_o (N x N) blocks
Forward OPT & zig-zag order
Block comparison and hash generation
Quantization and Entropy coding
Hash H_0
Compressed Image (I_c)
Receiver

Figure1: Hash generation at the sender

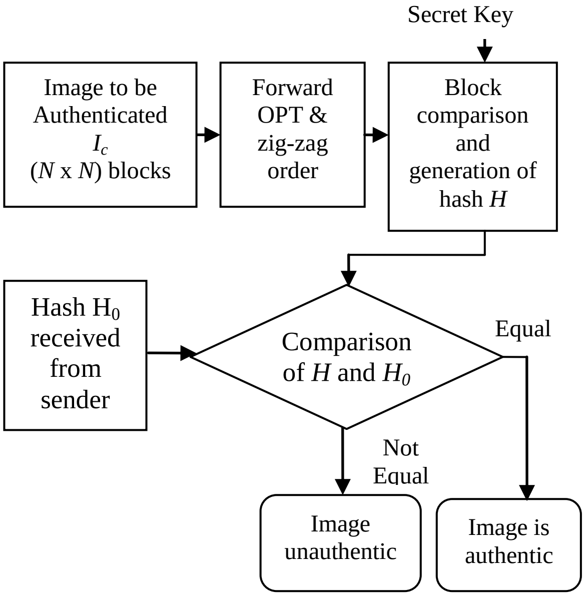

Secret Key
Image to be Authenticated I_c (N x N) blocks
Forward OPT & zig-zag order
Block comparison and generation of hash H
Hash H_0 received from sender
Comparison of H and H_0
Equal
Not Equal
Image unauthentic
Image is authentic

Figure 2: Hash verification at the receiver

In the following sub-sections, the hash generation and verification algorithms of the proposed inter-coefficient relationship based authentication scheme are presented.

4.1. Hash Generation Algorithm

The hash generation algorithm generates the hash by transforming the image into OPT domain and then selecting the block pairs using the secret key. After generating the hash value, the image is compressed and sent to the receiver along with the secret key and the computed hash in an encrypted form.

4.2. Hash Verification Algorithm

The verification algorithm decodes and de-quantizes the received compressed image and computes the hash by picking up the blocks pairs with same secret key used at the sender to generate the hash and verifies the authenticity of the received image by comparing it against the received hash.

In the following section the experimental results of the proposed system is presented.

5. Experimental Results

The proposed authentication system is tested with 50 grayscale images of different sizes. Some of the sample test images of size (128 x 128) with gray scale values in the range (0 – 255) are shown in Figure 3. This includes the images Lena, Peppers, Mandrill and other natural images. In the proposed scheme we first partition the test image into non-overlapping sub-blocks of size (4 x 4) and apply the proposed orthogonal polynomials based transformation as described in section 2 to obtain the transformed coefficients $\{\beta'_{ij} : 0 \le i < 4; 0 \le j < 4\}$. We then arrange the coefficients

Algorithm 1: Hash Generation

```
Input: Secret Key, Original Image $I_0$ to be authenticated, Compression quantization factor $CQ$.
Begin
1: Partition the original image into ($N$ x $N$) non-overlapping blocks. Repeat steps 2 to 7 for all the blocks.
2: Obtain the transformed blocks $\{\beta'_{ij:}\ 0 \le i < N; 0 \le j < N\}$ by applying the orthogonal polynomials based transformation described in section 2 and arrange the elements in 1- D zig-zag sequence.
3: Generate two sub-keys $k_1$ and $k_2$ from the secret key $sk$.
4: Generate random numbers using $k_1$ and select ($n$-1) AC coefficients from the first half of the 1-D sequence using the random numbers.
5: Form $b$ feature vectors using the DC coefficient and the selected AC coefficients, where $b$ is the number of blocks.
6: Generate pseudorandom sequence $\{s_1,s_2, s_b\}$ using $k_2$ where each $s_i$ denotes a feature vector. Form a mapping table $T$ with columns $P = \{s_1, s_3, ..., s_{b-1}\}$ and $Q = \{s_2, s_4, ..., s_b\}$.
7: Compare the elements of $P$ with $Q$ and generate hash as follows:
    (i) If $P_{ij} – Q_{ij} > = \tau$ then $h = 1$
    (ii) If $P_{ij} – Q_{ij} < \tau$ then $h = 0$
   where $0 \le i < b/2$ and $j = 0$ to 3 and $\tau$ is the tolerance value.
8: Concatenate the hash bits generated to form the final hash $H_0$.
9: Quantize all the OPT coefficients of all the blocks with $CQ$.
10: Perform entropy coding and obtain $I_c$.
End
Output: Compressed Image $I_c$.
        Hash $H_0$.
```

Algorithm 2: Hash Verification

```
Input
Secret Key.
Image $I_c$ to be authenticated.
Hash $H_0$.
Compression quantization factor $CQ$.
Begin
1: Perform entropy decoding and dequantization and partition $I_c$ into ($N$ x $N$) non-overlapping blocks. Repeat steps 2 and 3 for all the blocks.
2: Obtain the transformed blocks $\{\beta'_{ij:}\ 0 \le i < N; 0 \le j < N\}$ and arrange the elements in 1- D zig-zag sequence.
3: Generate the sub-keys $k_1$ and $k_2$ from the secret key $sk$ and perform steps 4 through 7 described in section 4.1.
4: Concatenate the hash bits generated to form the final hash $H$.
5: Compare the generated hash $H$ and $H_0$. If the hashes are equal then declare the image is to be authentic else declare the image to be unauthentic and return the tampered blocks.
End.
```

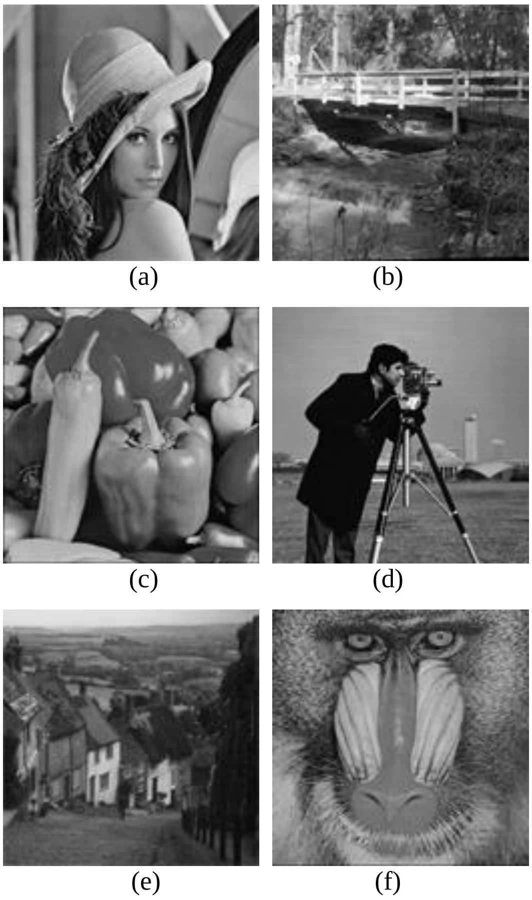
in 1-D zigzag sequence $\{\beta'_k : 0 \leq k < 16\}$. We then form the feature vectors by selecting the β'_0 coefficient and three β'_i s using a sub key k_1 generated from the secret key and then we generate the hash code by comparing the coefficients of selected vector pairs using the mapping table M, constructed based on the sub-key k_2 generated from the secret key, as described in sub-section 4.1. The image is then quantized as in the JPEG baseline system and entropy coded and sent to the receiver along with hash code generated. At the receiver the image is de-quantized, decoded and the hash code is computed using the same procedure employed by the sender. Then the computed hash code and the received hash code are compared. It is observed that the received image is declared to be authentic.

Next part of our experiment deals with the global distortions such as addition of noise and lossy compression. First we generate the hash code from the test images at the sender and then we apply global distortion before transmitting it to the receiver. Figures 4(a) and 4(b) shows the test images peppers and bridge after adding uniform noise (3%) and Gaussian noise (3%) respectively. The globally distorted image is transmitted to the receiver along with the hash code. Both the proposed scheme is able to successfully authenticate these images at the receiver. We then add 5% uniform noise and 5% Gaussian noise to the test images as shown in Figures 4(c) and 4(d). We observe that the proposed scheme indicates that these images are authentic. The responses of the proposed authentication scheme under additive noise are summarized in Table 1.

To demonstrate the robustness of the proposed scheme against lossy compression, the test images are compressed with quality factors 3, 5, 8 and 10 as shown in Figure 5(a) to Figure 5(d) respectively. The results produced by the authenticator are presented in the same Table I. We find that none of the image blocks of these compressed images are identified as unauthentic by the proposed scheme.

The performance of the proposed scheme is compared with the corresponding DCT based scheme by replacing OPT with DCT and the authentication results are incorporated in Table I. It was inferred that the DCT based scheme is able to tolerate only low additive noise (2%) in contrast to its OPT counterpart.

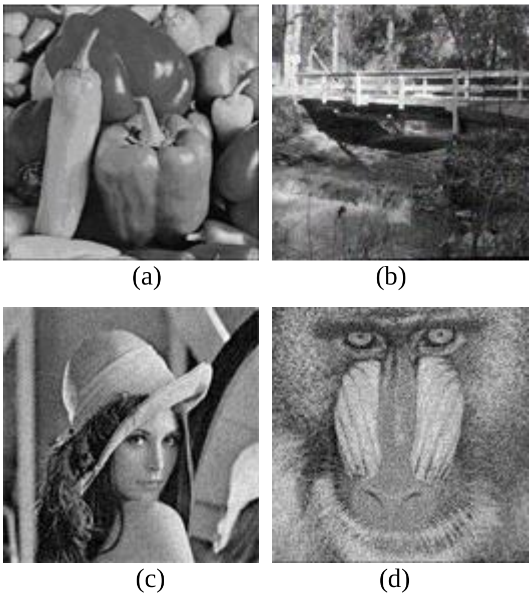
The last part of our experiment tests the effect of intentional tampering of the content. The test images intentionally tampered are shown in Figure 8 and the tampered areas are indicated by arrows. First, the text LENA is inserted in the Lena image as shown in Figure 6(a). Secondly, the window in the Gold Hill image is removed as shown in Figure 6(b). Thirdly, we cropped the center portion of the peppers image as shown in Figure 6(c) and finally, we slightly rotated the left eye in the Mandrill image. These tampered images are given as input to the authenticator. The proposed system raises alarms for these tampered images and the tampered block numbers are indicated signifying effective tamper localization capability.


(a) (b)

(c) (d)

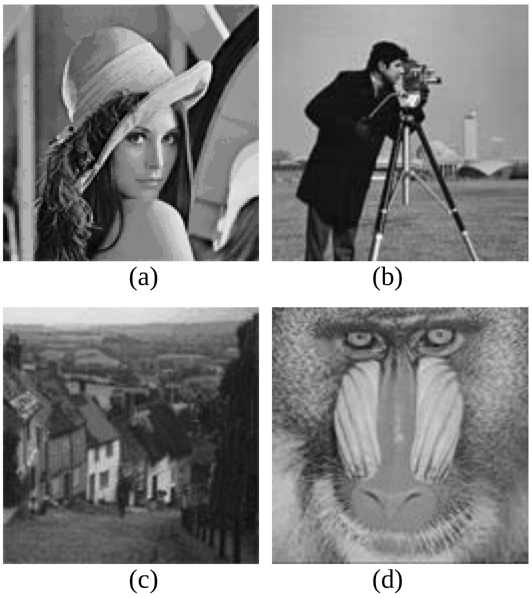
(e) (f)

Figure 3: Test Images (a) Lena (b) Bridge (c) Peppers (d) Cameraman (e) Gold Hill (f) Mandrill


(a) (b)

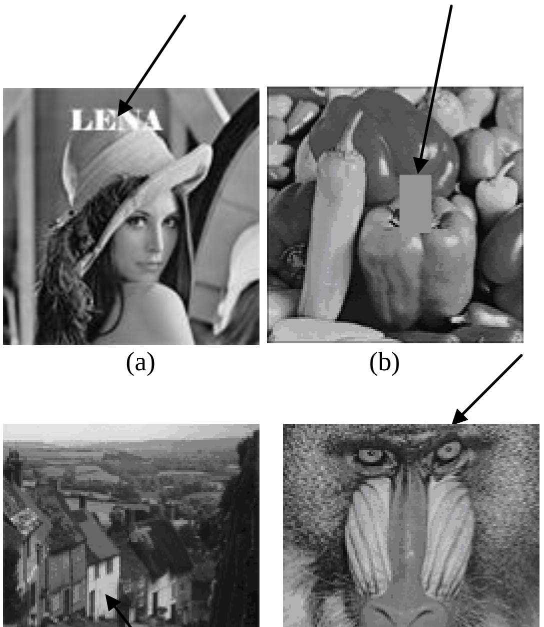
(c) (d)

Figure 4: Incidental distortions (a) Peppers with 3% uniform noise (b) Bridge with 3% Gaussian noise (c) Lena with 5% uniform noise (d) Mandrill with 5% Gaussian noise


(a) (b)

(c) (d)

Figure 5: Compressed Images (a) Lena (Quality Factor = 3) (b) Cameraman (Quality Factor = 5) (c) Gold Hill (Quality Factor = 8) (d) Mandrill (Quality Factor = 10).



(a) (b)

(c) (d)

Figure 6: Tampered test Images with tampered regions indicated by arrows.

Table 1: Results after incidental distortions on various test images

Image	Incidental distortions		Parameter	Authentication results	
				DCT based Scheme	OPT based Scheme
Lena	Compression	Low	QF = 3	A	A
Cameraman		Medium	QF = 5	A	A
Gold Hill		High	QF = 8	A	A
Mandrill		Max	QF = 10	A	A
Cameraman	Noise	Uniform	2%	A	A
Gold Hill		Gaussian	2%	A	A
Peppers		Uniform	3%	UA	A
Bridge		Gaussian	3%	UA	A
Lena		Uniform	5%	UA	A
Mandrill		Gaussian	5%	UA	A

QF- Quality Factor, A – Authentic, UA – Unauthentic

6 Conclusions

In this paper a semi-fragile image authentication system using the orthogonal polynomials based transformation is proposed. In this scheme the input image is first transformed using the orthogonal polynomials based transformation and the coefficients that form the feature vector are selected with a secret key. The system then exploits the inter-coefficient relationship between the orthogonal polynomial based transformed coefficients to form the hash code for authentication. From the experimental results it is evident that, the proposed scheme is effective in discriminating incidental distortions from intentional distortions. The proposed scheme is also compared with its DCT based counterpart and it is observed that the proposed scheme is more robust to additive noise than the DCT based scheme.

References

[1] F. Ahmed and M. Y. Siyal, "A secure and robust hashing scheme for Image Authentication," in *Proceedings of the IEEE International Conference on Information and Communication Systems (ICICS 2005)*, pp. 705-709, 2005.

[2] S. Bhattacharjee and M. Kutter, "Compression tolerant image authentication," *International Conference on Image Processing (ICIP'98)*, pp. 435-439, Chicago, USA, 1998.

[3] E. C. Chang, M. S. Kankanhalli, X. Guan, Z.g Huang and Y. Wu, "Robust image authentication using content based compression," *Multimedia Systems*, vol. 9, pp. 121-130, 2003.

[4] I. C. Chang, B. W. Hsu and C. S. Laih, "A DCT quatization-based authentication system for digital forensics," in *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE' 05)*, IEEE Computer Society, 2005.

[5] J. Fridrich and M. Goljan, *Protection of Digital Images Self Embedding*, Symposium on Content Security and Data Hiding in Digital Media, New Jersey Institute of Technology, New York, NJ, USA, 1999.

[6] J. Fridrich and M. Goljan, "Robust hash functions for digital watermarking," in *Proceedings of the IEEE International Conference on Information Technology – Coding and Computing' 00*, pp. 446-449, LAS Vegas, 2000.

[7] I. A. Ismail, M. Amin, and H. Diab, "A digital image encryption algorithm based on a composition of two chaotic logistic maps," *International Journal of Network Security*, vol. 11, no. 1, pp. 1-10, July 2010.

[8] R. Krishnamoorthi and P. Bhattacharayya, "A new data compression scheme using orthogonal polynomials," in *IEEE Proceedings on International Conference on Information, Communication and Signal Processing*, vol. 1, pp. 490-494, Nanyang Technology University, Singapore, 1997.

[9] R. Krishnamoorthi and P. D. S. K. Malarchelvi, "Selective combinational encryption of gray scale images using orthogonal polynomials based transformation," *International Journal of Computer Science and Network Security*, vol. 8, no. 5, pp. 195-204, 2008.

[10] I. S. Lee and W. H. Tsai, "Security protection of software programs by information sharing and authentication techniques using invisible ascii control codes," *International Journal of Network Security*, vol. 10, no. 1, pp. 1-10, 2010.

[11] C. Y. Lin and S. F. Chang, "Generating robust digital signature for image/ video authentication," in *Proceedings of Multimedia and Security Workshop at ACM Multimedia' 98*, pp. 49-53, Bristol, UK, 1998.

[12] C. Y. Lin and S. F. Chang, "A robust image authentication method distinguishing jpeg compression from malicious manipulation," *IEEE Transactions Circuits and Systems for Video Technology*, vol. 11, no. 2, pp.1453-1468, 2001.

[13] C. S. Lu and C. Y. Hsu, "Geometric distortion-resilient image hashing scheme and its applications on copy detection and authentication," *Multimedia Systems*, vol. 11, no. 2, pp. 159-173, 2004.

[14] C. Rey and J. L. Dugelay, "A survey of watermarking algorithms for image authentication," E*URASIP Journal on Applied Signal Processing*, vol. 6, pp. 613-621, 2002.

[15] S. V. Sathyanarayana, M. A. Kumar and K. N. Hari Bhat, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points," *International Journal of Network Security*, vol.12, no.3, pp.137-150, 2011.

[16] B. Schneier, *Applied Cryptography*, John Wiley and Sons, 1996.

[17] M. Schneider and S. F. Chang, "A Robust content-based digital signature for image authentication," in *International Conference on Image Processing*, pp. 227-230, Chicago, USA, 1998.

[18] J. J. Shen and P. W. Hsu, "A fragile associative watermarking on 2d barcode for data authentication," *International Journal of Network Security*, vol. 7, no. 3, pp. 301-309, 2008.

[19] Q. Sun and S. F. Chang, "A robust and secure media signature scheme for jpeg images," *Journal of VLSI Signal Processing*, vol. 41, pp. 305-317, 2005.

[20] A. Swaminathan, Y. and M. Wu, "Robust and secure image hashing," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 215-229, 2006.

[21] T. Uehara, R. Safavi-Naini and P. Ogunbona, "A secure and flexible authentication system for digital images," *Multimedia Systems*, vol. 9, pp. 441-456, 2004.

[22] R. Venkatesan, S. M. Koon, M. H. Jakubowski and P. Moulin, "Robust image hashing," in *Proceedings of IEEE Intenational Conference on Image Processing' 00*, pp. 664-666, Vancouver, 2000.

[23] 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. 1593-1601, 2001.

[24] L. Xie, G. R. Arce and R. F. Graveman, "Approximate message authentication codes," *IEEE Transactions on Multimedia*, vol. 3, no. 2, pp.242-252, 2001.

[25] S. Yu, Y. Hu and J. Zhou, "Content-based watermarking scheme for image authentication," in *Proceedings of the 8th International Conference on Control, Automation, Robotics and Vision*, pp. 1083-1087, Kunming, China, 2004.

P. D. Sheba Kezia Malarchelvi received B.E. in Computer Engineering in 1991 from Madurai Kamaraj University, Tamil Nadu, India. She completed M.E. in Computer Science in 1995 from the Regional Engineering College, Tiruchirappalli, Tamil Nadu, India. She received Ph.D. in Computer Science and Engineering in the year 2010 from Bharathidasan Institute of Technology, Bharathidasan University, Tamil Nadu, India. She has around 20 years of experience in teaching. Presently she is serving as Professor and Head of the Department of Computer Science and Engineering at J.J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India. Her research interests include Security, Grid Computing and Cloud Computing.