Available online at www.sciencedirect.com
ScienceDirect
Pattern Recognition 40 (2007) 1685–1694
PATTERN RECOGNITION
THE JOURNAL OF THE PATTERN RECOGNITION SOCIETY
www.elsevier.com/locate/pr

An invisible hybrid color image system using spread vector quantization neural networks with penalized FCM

Chi-Yuan Lin[a,*], Chin-Hsing Chen[b]

[a]*Department of Computer Science and Information Engineering, National Chin-Yi Institute of Technology, Taichung, 41111 Taiwan, ROC*
[b]*Department of Electrical Engineering, National Cheng Kung University, Tainan, 70101 Taiwan, ROC*

Received 4 February 2006; received in revised form 3 November 2006; accepted 8 November 2006

Abstract

In this paper, an invisible hybrid color image hiding scheme based on spread vector quantization (VQ) neural network with penalized fuzzy c-means (PFCM) clustering technology (named SPFNN) is proposed. The goal is to offer safe exchange of a color stego-image in the internet. In the proposed scheme, the secret color image is first compressed by a spread-unsupervised neural network with PFCM based on interpolative VQ (IVQ), then the block cipher Data Encryption Standard (DES) and the Rivest, Shamir and Adleman (RSA) algorithms are hired to provide the mechanism of a hybrid cryptosystem for secure communication and convenient environment in the internet. In the SPFNN, the penalized fuzzy clustering technology is embedded in a two-dimensional Hopfield neural network in order to generate optimal solutions for IVQ. Then we encrypted color IVQ indices and sorted the codebooks of secret color image information and embedded them into the frequency domain of the cover color image by the Hadamard transform (HT). Our proposed method has two benefits comparing with other data hiding techniques. One is the high security and convenience offered by the hybrid DES and RSA cryptosystems to exchange color image data in the internet. The other benefit is that excellent results can be obtained using our proposed color image compression scheme SPFNN method.

Keywords: Neural networks; PFCM; Vector quantization; Hadamard transforms; DES and RSA cryptosystems

1. Introduction

A cryptosystem is a useful tool for information security [1]. However, most traditional cryptosystems were only designed to protect text data. They are not suitable to encrypt image directly. Recently, there have been several cryptosystems proposed for gray image security [2–5]. Color images are widely used in our daily lives. A major issue for color image compression and security has been an explosive growth in the computers, networks, communications and multimedia applications.

In this paper, we focus on the subject of joint color image compression, color image encryption and hiding. In our presented color image hiding scheme, we employ a cover color image H to camouflage our secret color image S to a color stego-image F. The color stego-image F is one that can be made public. While illegal users steal it, most of them will think that this color stego-image F is an original.

Vector quatization (VQ) is a well-know image compression scheme [6–10]. VQ can provide a high compression ratio and better performance may be obtained than using any other block coding technique by increasing vector length and codebook size. The purpose of VQ is to create a codebook such that the average distortion between training vectors and their corresponding codevectors in the codebook is minimized.

Neural networks with gray relational and fuzzy clustering techniques have been demonstrated by the authors capable of performing VQ [11–13]. In this paper, we presented a spread neural network with penalized fuzzy c-means (PFCM) clustering technology (named SPFNN) based on interpolative

* Corresponding author. Tel.: +886 4 23924505; fax: +886 4 23917426.
E-mail addresses: chiyuan@ncit.edu.tw, cylin2.monica@msa.hinet.net (C.-Y. Lin).

0031-3203/$30.00
doi:10.1016/j.patcog.2006.11.004

VQ (IVQ) for color image compression. In the SPFNN, the PFCM is embedded into a two-dimensional competitive Hopfield neural network in order to generate an optimal solution for IVQ.

Furthermore, based on the presented scheme, we developed Data Encryption Standard (DES) software to encrypt compressed IVQ indices and sorted codebooks of secret color image information. Then the compressed and encrypted secret color image information was embedded into the frequency domain of the cover color image H by the Hadamard transform (HT).

DES is a famous and most widely used cryptosystem for commercial application today. Because DES is secure, no one can easily crush our cipher color image while they detect that this color stego-image F is a camouflage. Besides, the Rivest, Shamir, and Adleman (RSA) public-key system is hired to encrypt the symmetric key S_k of the DES cryptosystem so that our presented method is more secure, convenient and particularly suitable for the internet application.

The rest of this paper is organized as follows: Section 2 reviews the PFCM algorithm. In Section 3, we present our proposed scheme, which includes color image compression using a SPFNN based on IVQ, hybrid DES and RSA cryptosystem, HT and data embedding process. The data extracting process from the color stego-image is illustrated in Section 4. Empirical tests and security analysis are discussed in Section 5. Finally, conclusions are drawn in Section 6.

2. PFCM algorithm

Clustering is a process for classifying training samples in such a way that samples within a cluster are more similar to one another than samples belonging to different clusters. In many fields, such as segmentation, pattern recognition and vector quatization, clustering is an indispensable step.

The fuzzy c-means (FCM) clustering algorithm was first introduced by Dunn [14], the related formulations and algorithms were extended by Bezdek [15]. The FCM approach, like the conventional clustering techniques, minimizes an objective function in the least squared error sense. For class number c, sample number n and fuzzification parameter m ($1 \leqslant m < \infty$), the algorithm chooses $u_{i,j} : \mathbf{X} \to [0, 1]$ so that $\sum_{j=1}^{c} u_{i,j} = 1$ and $\boldsymbol{\omega}_j \in \mathbf{R}$ for $j = 1, 2, \ldots, c$ to minimize the objective function

$$J_{FCM} = \frac{1}{2} \sum_{j=1}^{c} \sum_{i=1}^{n} (u_{i,j})^m \|\mathbf{x}_i - \boldsymbol{\omega}_j\|^2, \tag{1}$$

where $u_{i,j}$ is the value of jth membership grade on ith sample $\mathbf{x}_i$. The cluster centroids $\boldsymbol{\omega}_1, \ldots, \boldsymbol{\omega}_j, \ldots, \boldsymbol{\omega}_c$ can be regarded as prototypes for the clusters represented by the membership grades. For the purpose of minimizing the objective function, the cluster centroids and membership grades are chosen so that a high degree of membership occurs for samples close to the corresponding cluster centroids.

Another strategy for fuzzy clustering, called the PFCM algorithm, with the addition of a penalty term was proposed by Yang [16,17]. It is a generalized FCM algorithm and was shown by Yang that the PFCM algorithm is more meaningful and effective than the FCM. The PFCM objective function is given by

$$\begin{aligned} J_{PFCM} &= \frac{1}{2} \sum_{j=1}^{c} \sum_{i=1}^{n} u_{i,j}^m \|\mathbf{x}_i - \boldsymbol{\omega}_j\|^2 - \frac{1}{2} v \sum_{j=1}^{c} \sum_{i=1}^{n} u_{i,j}^m \ln \alpha_j \\ &= J_{FCM} - \frac{1}{2} v \sum_{j=1}^{c} \sum_{i=1}^{n} u_{i,j}^m \ln \alpha_j, \end{aligned} \tag{2}$$

where α_j is a proportional constant of class j and $v(\geqslant 0)$ is a constant. The penalty term $-\frac{1}{2} v \sum_{j=1}^{c} \sum_{i=1}^{n} u_{i,j}^m \ln \alpha_j$ is added to the objective function, when $v = 0$, J_{PFCM} equals to J_{FCM}. α_j, $\boldsymbol{\omega}_j$, and $u_{i,j}$ are defined as

$$\alpha_j = \frac{\sum_{i=1}^{n} u_{i,j}^m}{\sum_{j=1}^{c} \sum_{i=1}^{n} u_{i,j}^m}, \quad j = 1, 2, \ldots, c, \tag{3}$$

$$\boldsymbol{\omega}_j = \frac{1}{\sum_{i=1}^{n} (u_{i,j})^m} \sum_{i=1}^{n} (u_{i,j})^m \mathbf{x}_i \tag{4}$$

and

$$u_{i,j} = \left(\sum_{\ell=1}^{c} \frac{(\|\mathbf{x}_i - \boldsymbol{\omega}_j\|^2 - v \ln \alpha_j)^{1/(m-1)}}{(\|\mathbf{x}_i - \boldsymbol{\omega}_\ell\|^2 - v \ln \alpha_\ell)^{1/(m-1)}} \right)^{-1}. \tag{5}$$

The steps of the PFCM algorithm are given in the Appendix.

3. Invisible hybrid color image hiding system

In this paper, the proposed scheme is a combination between color image compression using our presented SPFNN method and a hybrid color image cryptosystem using the DES and RSA cryptosystems.

An image hiding scheme must be extremely secure to the insecure communication channel, and at the same time not reduce the visual quality of the color stego-image F when the secret color image S is concealed, so we presented a new SPFNN based on IVQ for color image compression scheme. To enhance the color image security problem, we implement DES and RSA algorithms so that the design of a high security color image hybrid cryptosystem becomes feasible. The relevant illustrations are described as follows.

3.1. Color image compression using SPFNN based on IVQ

Suppose an image is divided into n blocks (vectors of pixels) and each block occupies $\ell \times \ell$ pixels. A vector quantizer maps the Euclidean $\ell \times \ell$-dimensional space $\mathbf{R}^{\ell \times \ell}$ into a set $\{\boldsymbol{\omega}_j, j=1, 2, \ldots, c\}$ of points in $\mathbf{R}^{\ell \times \ell}$, called a codebook. A vector quantizer approximates a training vector with least distortion by one of the codevectors in the codebook. The average distortion $E[d(\mathbf{x}_i, \boldsymbol{\omega}_j)]$ between an input sequence

of training vectors $\{\mathbf{x}_i, j = 1, 2, \ldots, n\}$ and its corresponding output sequence of codevectors $\{\boldsymbol{\omega}_j, j = 1, 2, \ldots, c\}$ is defined as

$$D = E[d(\mathbf{x}_i, \boldsymbol{\omega}_j)] = \frac{1}{n}\sum_{i=1}^{n} d(\mathbf{x}_i, \boldsymbol{\omega}_j). \tag{6}$$

The distortion measure $d(\mathbf{x}_i, \boldsymbol{\omega}_j)$ is defined as the squared Euclidean distance between vectors $\mathbf{x}_i$ and $\boldsymbol{\omega}_j$. A vector quantizer is optimal if the average distortion is at the minimum value.

The Hopfield neural network with simple architecture and parallel potential has been applied in many fields [18–21]. In this paper, the authors applied the Hopfield neural network with the penalized fuzzy c-means strategy (named PFNN) to VQ.

For n training vectors and c classes, the PFNN consists of $n \times c$ neurons, which can be conceived as a two-dimensional array. Each vector is iteratively trained to update the neurons' weights by using the nearest neighbor rule.

The proposed method assigns each training vector to a class in such a manner that the average distortion between the training vectors to their associated class centers (or codevectors) is minimized. Iteratively updating the synaptic weights of the neural interconnections will gradually force the network to converge into a stable state at which the energy function of the system is minimized. By the within-class scatter matrix criteria, the optimization problem can be mapped into a two-dimensional Hopfield neural network with the PFCM strategy. Instead of using the competitive learning strategy, the PFNN use the PFCM algorithm to eliminate the need for finding weighting factors in the energy function.

Let $u_{i,j}$ be the fuzzy state of the (i, j)th neuron and $\mathbf{W}_{i,j;k,j}$ represents the interconnected weight between neuron (i, j) and neuron (k, j). A neuron (i, j) in the network receives weighted inputs $\mathbf{W}_{i,j;k,j}$ from each neuron (k, j) and a bias $\mathbf{I}_{i,j}$ from outside. The total input to neuron (i, j) is computed as

$$Net_{i,j} = \left\| \mathbf{x}_i - \sum_{k=1}^{n} \mathbf{W}_{i,j;k,j}(u_{k,j})^m \right\|^2 + \mathbf{I}_{i,j}. \tag{7}$$

The modified Lyapunov energy function of the two-dimensional Hopfield neural network using PFCM strategy is given by

$$E = \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{c}(u_{i,j})^m \left\| \mathbf{x}_i - \sum_{k=1}^{n} \mathbf{W}_{i,j;k,j}(u_{k,j})^m \right\|^2 + \sum_{i=1}^{n}\sum_{j=1}^{c} \mathbf{I}_{i,j}(u_{i,j})^m, \tag{8}$$

where $\sum_{k=1}^{n}\mathbf{W}_{i,j;k,j}$ is the total weighted input received from neuron (k, j) in row j, $u_{i,j}$ is the output state at neuron (i, j), and m is the fuzzification parameter. Each column of this modified Hopfield network represents a codevector (class) and each row represents a training vector. The network reaches a stable state when the modified Lyapunov energy function is minimal. For example, a neuron (i, j) in a maximum membership state indicates that the training vector $\mathbf{x}_i$ belongs to class j.

In order to generate an adequate classification with constraints, the objective function is given by

$$E = \frac{A}{2}\sum_{i=1}^{n}\sum_{j=1}^{c}(u_{i,j})^m \left\| x_i - \sum_{k=1}^{n} \frac{1}{\sum_{h=1}^{n}(u_{h,j})^m}\mathbf{x}_k(u_{k,j})^m \right\|^2 + \frac{B}{2}\left| \left(\sum_{i=1}^{n}\sum_{j=1}^{c} u_{i,j}\right) - n \right|^2 - v\sum_{i=1}^{n}\sum_{j=1}^{c}(u_{i,j})^m \ell n(\alpha_j). \tag{9}$$

The first term in Eq. (9) is the within-class scatter energy that is the average distance between training vectors to the cluster centroid over c clusters. The second term guarantees that the n training vectors in $\mathbf{X}$ can only be distributed among these c classes. More specifically, the second term imposes constraints on the objective function and the first term minimizes the intra-class Euclidean distance from the training vectors to the cluster centroid in any given cluster. The last term is the penalized term as given in Eq. (2) of the PFCM algorithm.

As mentioned in Ref. [18], the quality of the classification result is very sensitive to the weighting factors A and B. Searching for optimal values for these weighting factors is time-consuming and laborious. To alleviate this problem, a two-dimensional Hopfield neural network with PFCM clustering strategy is proposed so that the constrain terms can be handled more efficiently. In PFNN, all the neurons in the same row compete one another to determine which neuron has the maximum membership value belonging to class j. The summation of the membership grade of states in the same row equals 1, and the total membership states in all n rows equal n. It is also ensured that all training vectors will be classified into these c classes. The modified Hopfield neural network PFNN enables the scatter energy function to converge rapidly to a minimum value. By using the PFCM strategy, the scatter energy of the PFNN can be simplified as

$$E = \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{c}(u_{i,j})^m \left\| \mathbf{x}_i - \sum_{k=1}^{n} \frac{1}{\sum_{h=1}^{n}(u_{h,j})^m}\mathbf{x}_k(u_{k,j})^m \right\|^2 - v\sum_{i=1}^{n}\sum_{j=1}^{c}(u_{i,j})^m \ell n(\alpha_j). \tag{10}$$

The minimization of energy E in Eq. (10) is greatly simplified since it contains only two terms and hence the need to determine the weighting factors A and B vanishes. By comparing Eq. (10) with the modified Lyapunov function

Eq. (8), the synaptic interconnection weights and the bias input can be obtained as

$$\mathbf{W}_{i,j;k,j} = \frac{1}{\sum_{h=1}^{n}(u_{h,j})^m}\mathbf{x}_k, \tag{11}$$

and input bias

$$\mathbf{I}_{i,j} = -v\ell n(\alpha_j). \tag{12}$$

By introducing Eqs. (11) and (12) into Eq. (7), the input to neuron (i, j) can be expressed as

$$Net_{i,j} = \left\| x_i - \sum_{k=1}^{n} \frac{1}{\sum_{h=1}^{n}(u_{h,j})^m}\mathbf{x}_k(u_{k,j})^m \right\|^2 - v\ell n(\alpha_j). \tag{13}$$

From Eqs. (4), (5) and (13), the state (i.e., membership function) of the neuron at the (i, j)th row is given as

$$u_{i,j} = \left[\sum_{\ell=1}^{c}\left(\frac{Net_{i,j}}{Net_{i,\ell}}\right)^{1/(m-1)}\right]^{-1} \quad \text{for all } j. \tag{14}$$

By using Eqs. (13) and (14), the PFNN can classify the training vectors into c classes in a parallel manner. We then map the R, G, and B plane training vectors of a color image to the spread PFNN (named SPFNN) neuron array that compress them separately by treating each color plane as a single gray-level image. Therefore, the SPFNN based vector quatizer in the pth plane can be modified as follows:

SPFNN Algorithm

Step 1: Input a set training vector $\mathbf{X}_p = \{\mathbf{x}_{1;p}, \mathbf{x}_{2;p}, \ldots, \mathbf{x}_{n;p}\}$, constant $v(v > 0)$, fuzzification parameter $m(1 \leqslant m < \infty)$, the number of class c, and initialize the states for all neurons $U = [u_{i,j;p}]$ (membership matrix).

Step 2: Compute $\alpha_{j;p}$ and the weighted matrix using Eqs. (3) and (11), respectively.

Step 3: Calculate the input to each neuron (i, j) by Eq. (13)

$$Net_{i,j;p} = \left\| \mathbf{x}_{i;p} - \sum_{k=1}^{n} \frac{1}{\sum_{h=1}^{n}(u_{h,j;p})^m}\mathbf{x}_{k;p}(u_{k,j;p})^m \right\|^2 - v\ell n(\alpha_{j;p}).$$

Step 4: Apply Eq. (14) to update the neurons' membership values in a synchronous manner:

$$u_{i,j;p} = \left[\sum_{\ell=1}^{c}\left(\frac{Net_{i,j;p}}{Net_{i,\ell;p}}\right)^{1/(m-1)}\right]^{-1} \quad \text{for all } j.$$

Step 5: Compute $\Delta = \max(|U^{(t+1)} - U^{(t)}|)$, If $\Delta > \varepsilon$ go to Step 2, otherwise go to Step 6.

Step 6: Find the codebook for the final membership matrix in the pth plane $(p = 1, 2, 3)$.

Furthermore, IVQ has been devised to alleviate the visible block structure of coded images and lessen the sensitive codebook problems produced by a simple vector quantizer [22]. In a VQ system, the complexity of the encoders is often depending on the size of the codebook used. In this paper, for the purpose of enhancing the imperceptibility of the color stego-image F, the $N \times N$ secret color image S was down-sampled into $(N \times N)/2$ size image. Therefore, just only $(N \times N)/2$ pixels of each plane in the secret color image S was processed using the proposed SPFNN approach. Then the interpolative method was used to rebuild the empty pixels using the average of their neighbor pixels in each plane. That is to say, the interpolative method must do extra work to interpolate the pixels. Consequently, the rebuilt quality maybe reduced somewhat, but it can reduce partly hiding data for the purpose of enhancing the imperceptibility of the color stego-image F.

3.2. Hybrid cryptosystem based on DES and RSA

In our invisible hybrid color image hiding system, the sender uses the symmetric key S_k to the DES color image information encryption process and the password *psw* to generate the *PN* sequence used in the embedding process. On the other hand, the receiver uses *rndkey* by the RSA public-key cryptosystem to recover the symmetric key S_k to DES color decryption process and *rndsed* by RSA public-key cryptosystem to recover the password *psw* used to generate the same *PN* sequence in the retrieving process. The relevant illustrations are described as follows.

3.2.1. DES private-key cryptosystem

The DES is the well known and the first standardized algorithm, which was first introduced in 1977 by the US National Bureau of Standards [23]. DES can encrypt and decrypt 64-bit data blocks with a 56-bit symmetric key S_k.

Fig. 1 sketches the DES algorithm [24]. Each of the 16 iterations is identical in logic but uses a different key. The operations are formulated as follow:

- First, a block of the 64 bit permuted data is divided into a left sub-block L_{r-1} and a right sub-block R_{r-1} of 32 bits each.
- The leftmost 32 bit of the input block is simply a duplicate of the rightmost 32 bit.
- The rightmost 32 bit of the input block R_{r-1} is expanded to a 48 bit block using the bit expansion table.
- The 56 bit S_k is used to generate a 48 bit round keys K_r by key scheduling, where $1 \leqslant r \leqslant 16$.
- The 48 bits round key and the 48 bits data block are XORed together. The result is divided into eight groups of 6 bits each, each of which is passed through a different 'S-box' to produce eight 4 bits groups. They are concatenated together to form 32 bit output.
- The resulting 32 bits are then passed through a fixed permutation. The new 32 bits block and the leftmost 32 bit of L_{r-1} are XORed together to form the rightmost 32 bit of R_r.

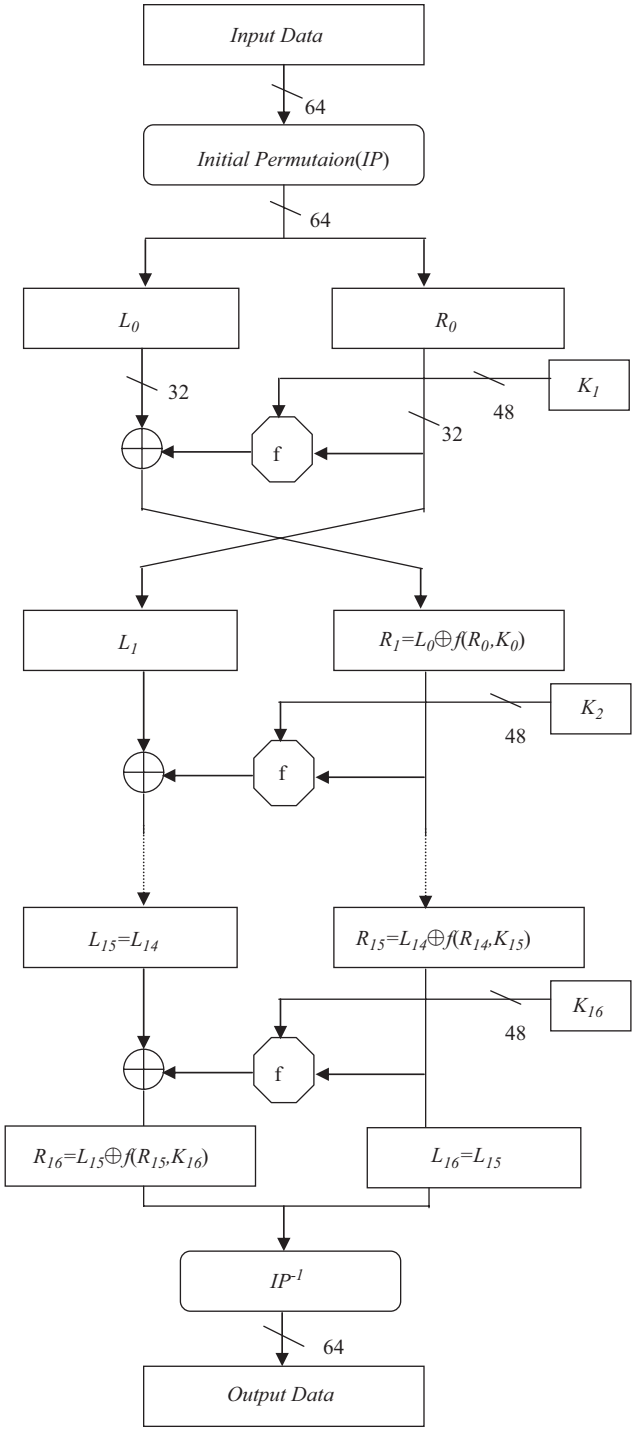

Fig. 1. The flowchart of the DES algorithm.

Summarized, the encryption process is as follows:

$$L_r = R_{r-1}, \tag{15}$$

$$R_r = L_{r-1} \oplus f(R_{r-1}, K_r). \tag{16}$$

Then the decryption process is the same encryption process but using round keys for the decryption in the reverse order.

3.2.2. RSA public-key cryptosystem

In 1976, Diffie and Hellman proposed the concept of public key cryptography [25]. In 1978 Rivest, Shamir and Adleman proposed the RSA public-key cryptosystem [26]. Unlike symmetric cryptosystems, public-key cryptosystems use two distinct keys. It is possible to communicate securely without any prior relationship or secret key exchange between parties. The RSA scheme is a block cipher where each block is an integer between 0 and no-1 for some no. In encryption, a plaintext message S_k and psw are encrypted to its ciphertext $rndkey$ and $rndsed$ by

$$rndkey = S_k^e \bmod no, \tag{17}$$

$$rndsed = psw^e \bmod no. \tag{18}$$

In decryption, the plaintext S_k and psw are restored using

$$S_k = rndkey^d \bmod no, \tag{19}$$

$$psw = rndsed^d \bmod no. \tag{20}$$

In Eqs. (17)–(20), where (e, no) is the encryption key (public key), and (d, no) is the decryption key (private key), respectively. The RSA key pair (e, d) can be found as follows. First, we randomly chose two large prime numbers p, q, and $no = p \times q$ (which should be discard after the key generation process is complete). Then find e such that $GCD((p-1)(q-1), e) = 1$ where $1 < e < (p-1)(q-1)$ and $de = 1 \bmod (p-1)(q-1)$. However, to find the key pair is infeasible.

3.3. Hadamard transform and data embedding process

Among various popular image transforms, HT [27,28] takes the least computation overhead since its basis vectors contain only $+1$ and -1. No multiplication is necessary and only fixed point arithmetic is required for computing the transformation. The forward and inverse two-dimensional HT for an $N \times N$ image can be defined as

Forward:

$$F(u, v) = \frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} f(j, k)(-1)^{\sum_{i=0}^{\ell-1}[b_i(u)b_i(j)+b_i(v)b_i(k)]}. \tag{21}$$

Inverse:

$$f(j, k) = \frac{1}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} F(u, v)(-1)^{\sum_{i=0}^{\ell-1}[b_i(u)b_i(j)+b_i(v)b_i(k)]}, \tag{22}$$

where $F(u, v)$ are the HT coefficients, $f(j, k)$ are the pixel value at (j, k), $N = 2^\ell$ for some ℓ, and $b_i(u)$ is the ith bit of u in the binary form.

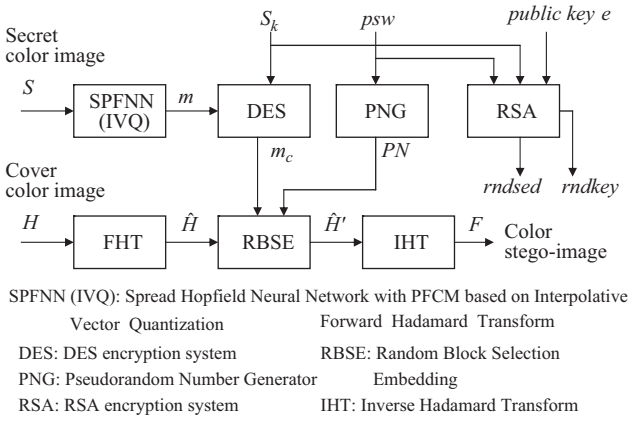

Fig. 2. The flowchart of the embedding process.

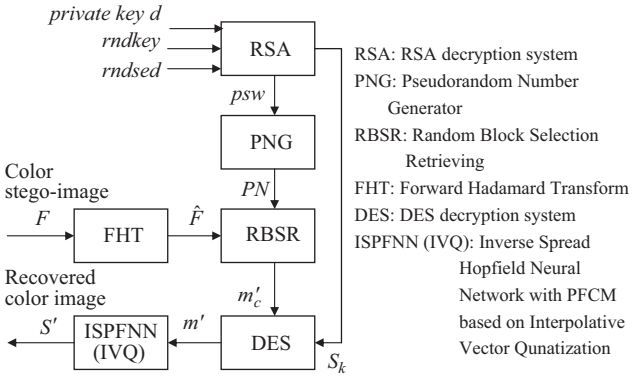

Fig. 3. The flow chart of the recovering process.

The overall concealing process of our proposed scheme is shown in Fig. 2. The secret color image S was encoded by our proposed SPFNN based on IVQ into indices bit stream $\{m\}$. A DES private-key cryptosystem was used to encrypt $\{m\}$ into $\{m_c\}$ to enhance security. On the other hand, the cover color image H is divided into non-overlapped blocks, which are forward HT (FHT) transformed to $\hat{H}$. In the embedding process, the bit 3 of eight coefficients of one randomly selected block by the PN sequence is used for embedding the same number of bit stream $\{m_c\}$ until all bit stream $\{m_c\}$ is run out. The resultant image $\hat{H}'$ after the embedding process is then inversely transformed to obtain the color stego-image F by the inverse HT (IHT).

4. Data recovering process

A process which inverses the concealing process is used to recover the secret color image S. The flow chart of the recovering process is shown in Fig. 3. The color stego-image F is transformed to $\hat{F}$ by FHT. The PN sequence used in the concealing process is used to select the embedded block from $\hat{F}$. All the retrieved bit sequence $\{m'_c\}$ is then decrypted by DES into $\{m'\}$. By rebuilding process through inverse SPFNN (ISPFNN) based on IVQ, the secret color image S' is recovered.

5. Empirical tests and security analysis

According to the proposed scheme, and the human visual system, some amount of distortion is allowed. In this paper, we developed a new SPFNN algorithm based on IVQ to compress secret color image S and combined the DES private-key cryptosystem and the RSA public-key cryptosystem to offer safe exchange of a color stego-image F in the internet. The relative compression efficiency, concealing empirical test, and security analysis are shown as follows.

5.1. Compression efficiency

Codebook design is the primary problem in image compression based on VQ. In this paper, the qualities of the images reconstructed from the PFNN method were compared with the conventional VQ method LBG. The size of the training image is 256×256 with 8-bit gray level, which is divided into 4×4 blocks to generate 4096 non-overlapping 16-dimensional training vectors. Three codebooks of size 64, 128, and 256 were built using this training data. The compression rates were $\frac{6}{16}=0.375$, $\frac{7}{16}=0.438$, and $\frac{8}{16}=0.5$ bits per pixel, respectively. The resulting images were evaluated by the peak signal to noise ratio (PSNR) defined as

$$PSNR = 10 \log_{10} \frac{255 \times 255}{e^2}, \tag{23}$$

where e^2 is the mean squared of the reconstructed image error and 255 is the peak gray level, respectively. Table 1 summarizes the quality of the codebook design for various parameter m, and v by PFNN in 20 iterations. Table 1 indicates that the quality is best when parameter $m=1.2$. Table 2 shows the performances for the typical VQ (LBG) and the proposed PFNN with parameter $m = 1.2$ and $v = 1.1$ for various images with the codebook size $c = 128$. According to Table 2, the average $PSNR$ from PFNN are about 2.25 dB higher than those from the conventional LBG method.

In the color compression simulation, the original color image was separated into RGB three-plane. Then each plane was trained using the proposed SPFNN method to generate better codebook based on VQ. To show the reconstruction performance, the resulting images were evaluated by the average $PSNR$ among the three-color planes by

$$PSNR_A = \frac{PSNR_R + PSNR_G + PSNR_B}{3}, \tag{24}$$

where $PSNR_R$, $PSNR_G$, and $PSNR_B$ are the $PSNR$ for red, green, and blue planes, respectively. The$PSNRs$ of the "F16", "Girl", and "Couple" images calculated during the experiments are shown in Table 3, and the reconstructed images using the SPFNN with 128 codevectors each plane are shown

Table 1
PSNR of the Pepper and Baboon images from codebook size $c = 128$ designed by the various parameter m and v for the proposed PFNN algorithm in 20 iterations

v/Images		m					
		1.1	1.2	1.3	1.5	1.7	1.9
1.1	Pepper	26.683	27.225	26.590	25.539	22.661	22.071
	Baboon	23.932	23.479	22.160	21.422	21.308	21.271
1.2	Pepper	26.758	27.202	26.600	25.512	22.654	22.067
	Baboon	23.937	23.476	22.151	21.419	21.308	21.271
1.3	Pepper	26.780	27.230	26.590	25.477	22.640	22.062
	Baboon	23.938	23.473	22.141	21.417	21.308	21.270
1.5	Pepper	26.770	27.196	26.560	25.355	22.611	22.052
	Baboon	23.943	23.468	22.170	21.413	21.307	21.268
1.7	Pepper	26.735	27.213	26.536	25.286	22.606	22.041
	Baboon	23.959	23.460	22.099	21.409	21.306	21.265
1.9	Pepper	26.638	27.242	26.506	25.253	22.583	22.030
	Baboon	23.941	23.453	22.078	21.405	21.306	21.264

Table 2
Comparison of the various gray test images coded results using the LBG and PFNN methods

Test images	Methods	PSNR (dB)	Bit rate (bit/pixel)
F16	LBG	25.291	0.438
	PFNN	26.889	0.438
Girl	LBG	28.512	0.438
	PFNN	30.694	0.438
Couple	LBG	29.403	0.438
	PFNN	31.626	0.438
Pepper	LBG	25.293	0.438
	PFNN	27.568	0.438

Table 3
PSNRs of the various color test images reconstructed by the SPFNN with 128 codevectors each plane

Test images	Plane			Average
	R	G	B	
F16	28.289	27.247	31.257	28.931
Girl	29.988	30.581	30.257	30.275
Couple	30.793	31.651	31.581	31.342

in Fig. 4. Similarly, from the simulated results, the proposed SPFNN method can produce good reconstructed color image quality.

5.2. Concealing empirical test

To show the feasibility of the proposed scheme, we employed the 256×256 "Girl" and "Couple" color images as our secret color images. To camouflage these secret color images, we employed the 256×256 "Sailboat" and "Tree" color images as the cover color images. Fig. 5 shows the compressed IVQ indices and sorted codebooks images and their DES encrypted images of the "Girl" and "Couple" secret color images. Fig. 6 shows the concealing and recovering empirical test results. Figs. 6(a) and (b) show the "Sailboat" color stego-image and the recovered "Girl" secret color image, respectively. Figs. 6(c) and (d) show the "Tree" color stego-image and the recovered "Couple" secret color image, respectively. The *PSNR* of the color stego-image F and color cover image H, and the *PSNR* of the secret color image S and recovered secret color image S', both cases are shown in Tables 4 and 5, respectively. According to Table 4 and Figs. 6(a) and (c), the "Sailboat" and "Tree" color stego-images whose average PSNRs are 38.978 and 38.890 dB, respectively. Another, according to Table 5 and Figs. 6(b) and (d), the "Girl" and "Couple" secret color images recovered whose average PSNRs are 29.066 and 29.802 dB, respectively. Empirical test results show that the color stego-images are unobtrusiveness and the retrieved and reconstructed secret color images have well-acceptable quality.

5.3. Security analysis

In our invisible hybrid color image hiding system, a cover color image H is used to camouflage a secret color image S to form a color stego-image F. Since the distortion between H and F is insignificant, an illegal user cannot sense and hint in the F, even he possesses it. Furthermore, our hiding scheme employed several security techniques to protect color images from attacks. The security issue of our system is analyzed as follows:

1. The presented SPFNN based on IVQ coding technique is employed to compress the S into indices & sorted codebooks and encrypt them by the DES cryptosystem, which is famous and secure. The effective S_k is 56 bits, and then it has 2^{56} possible combinations. Any illegal user wants to break it needs to make 2^{56} tries to break the S_k.
2. In the embedding process, the $N \times N$ cover color image H was divided into $((N \times N) \div (\ell \times \ell))$ non-overlapping

Fig. 4. “Girl” and “Couple” color test images, reconstructed images using the spread PFNN with 128 codevectors each plane, and their local enlarged images for the original and compressed images: original images (left), reconstructed images (right).

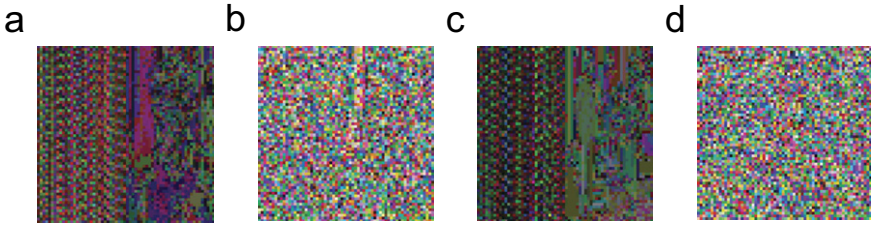

Fig. 5. The compressed IVQ indices & sorted codebooks and their DES encrypted images of the “Girl” and “Couple” secret color images: (a) IVQ indices and sorted codebook image of the “Girl” secret color image, (b) DES cipher image of the compressed “Girl” secret color image, (c) IVQ indices and sorted codebook image of the “Couple” secret color image and (d) DES cipher image of the compressed “Couple” secret color image.

Fig. 6. Empirical tests for the proposed scheme: (a) the "Sailboat" color stego-image, (b) the "Girl" secret color image recovered, (c) the "Tree" color stego-image and (d) the "Couple" secret color image recovered.

Table 4
The *PSNR* of the color stego-image F and cover color image H

Cover color image	Secret color image	R	G	B	Average
Sailboat	Girl	39.099	38.932	38.903	38.978
Tree	Couple	38.785	38.966	38.920	38.890

Table 5
The *PSNR* of the secret color image S and recovered secret color image S'

Test images	Plane			Average
	R	G	B	
Girl	28.808	29.275	29.116	29.066
Couple	29.234	30.155	30.018	29.802

$(\ell \times \ell)$ HT Blocks. The proper block which is embedded is decided by the *PN* sequence. However, the *PN* sequence is generated by the random number seed of the secret key, an illegal user will need $((N \times N) \div (\ell \times \ell))!$ tries to break the key.

3. The RSA public-key cryptosystem is based on the difficulty of the factorizing large integers [26], which is very hard to solve even now. The RSA cryptosystem used in our scheme enhances the convenience and security for the internet.

6. Conclusions and future work

In this paper, we proposed a novel color image hiding technique that is invisible while a big color image is concealed in a cover color image. Same as other systems, imperceptibility and security are essentially compromised in ours. Nevertheless, there are two benefits of our system over others. One is the highly secure and convenient offered by hybrid DES and RSA cryptosystems to exchange color image data in the internet. The other is excellent results can be obtained through our proposed new spread-unsupervised scheme based on the competitive Hopfield neural network with PFCM for color image compression. Due to the SPFNN's highly interconnected and parallel abilities, computation time can be largely reduced by way of parallel processing. The design of a dedicated hardware of SPFNN is currently under investigation.

Appendix

PFCM Algorithm

Step 1: Initialize the cluster centroids $\boldsymbol{\omega}_j (2 \leqslant j \leqslant c)$, $v (v > 0)$, fuzzification parameter $m (1 \leqslant m < \infty)$, and the value $\varepsilon > 0$. Give a fuzzy c-partition $U^{(0)}$ and $t = 1$.

Step 2: Calculate the $\alpha_j^{(t)}$, $\boldsymbol{\omega}_j^{(t)}$ with $U^{(t-1)}$ using Eqs. (3) and (4).

Step 3: Calculate the membership matrix $U^{(t)} = [u_{i,j}]$ with $\alpha_j^{(t)}$, $\boldsymbol{\omega}_j^{(t)}$ using Eq. (5).

Step 4: Compute $\Delta = \max(|U^{(t+1)} - U^{(t)}|)$. If $\Delta > \varepsilon$, $t = t + 1$ and go to Step 2; otherwise go to Step 5.

Step 5: Find the results for the final class centroids.

References

[1] D.E.R. Denning, Cryptography and Data Security, Addison-Wesley, Reading, MA, 1983.

[2] N. Bourbakis, C. Alexopoulos, Picture data encryption using scan patterns, Pattern Recognition 25 (1992) 567–581.

[3] T.S. Chen, C.C. Chang, M.S. Hwang, A virtual image cryptosystem based upon vector quantization, IEEE Trans. Image Processing 7 (10) (1998) 1485–1488.

[4] P.P. Dang, P.M. Chau, Image encryption for secure internet multimedia applications, IEEE Trans. Consumer Electron. 46 (3) (2000) 395–403.

[5] C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption algorithm for image cryptosystems, J. Syst. Software (2001) 83–91.

[6] Y. Linde, A. Buzo, R.M. Gray, An algorithm for vector quantizer design, IEEE Trans. Commun. COM-28 (1980) 85–94.

[7] R.M. Gray, Vector quantization, IEEE ASSP Mag. 1 (1984) 4–29.

[8] A. Gersho, R.M. Gray, Vector Quantization and Signal Compression, Kluwer Academic Publishers, Norwell, MA, 1992.

[9] E.A. Riskin, T. Lookabaugh, P.A. Chou, R.M. Gray, Variable rate vector quantization for medical image compression, IEEE Trans. Med. Imaging 9 (1990) 290–298.

[10] E. Yair, K. Zeger, A. Gersho, Competitive learning and soft competition for vector quantizer design, IEEE Trans. Signal Process. 40 (1992) 294–309.

[11] C.Y. Lin, C.H. Chen, Color image compression using spread grey-based neural networks in the transform domain, Proceedings of the 19th Workshop on Combinatorial Mathematics and Computation theory, 2002, pp. 137–145.

[12] C.Y. Lin, C.H. Chen, A genetic grey-based neural networks with wavelet transform for search of optimal codebook, IEICE Trans. Fundam. E86-A (3) (2003) 715–721.

[13] C.Y. Lin, C.H. Chen, R.M. Chen, A spread neural network with fuzzy clustering technique applied to color image coding in the MDT domain, IEEE Proceedings on the Ninth International Conference on Parallel and Distributed Systems, 2002, pp. 583–588.

[14] J.C. Dunn, A fuzzy relative of the ISODATA process and its use in detecting compact well-separated clusters, J. Cybern. 3 (3) (1974) 32–57.

[15] J.C. Bezdek, Fuzzy mathematics in pattern classification, Ph.D. Dissertation, Applied Mathematics, Cornell University, Ithaca, New York, 1973.

[16] M.S. Yang, On a class of fuzzy classification maximum likelihood procedures, Fuzzy Sets and Systems 57 (1993) 365.

[17] M.S. Yang, C.F. Su, On parameter estimation for normal mixtures based on fuzzy clustering algorithms, Fuzzy Sets and Systems 68 (1994) 13.

[18] P.C. Chung, C.T. Tsai, E.L. Chen, Y.N. Sun, Polygonal approximation using a competitive Hopfield neural network, Pattern Recognition 27 (1994) 1505–1512.

[19] K.S. Cheng, J.S. Lin, C.W. Mao, The application of competitive Hopfield neural network to medical image segmentation, IEEE Trans. Med. Imaging 15 (1996) 560–567.

[20] R.M. Chen, Y.M. Huang, C.Y. Lin, Competitive neural network to solve real-time scheduling, International Computer Symposium, 2002, pp. 1–8.

[21] C.Y. Lin, C.H. Chen, Image compression using grey-based Hopfield neural network and block truncation coding, Proceedings of the 20th Workshop on Combinatorial Mathematics and Computation Theory, 2003, pp. 193–198.

[22] H.M. Hang, B.G. Haskell, Interpolative vector quantization of color images, IEEE Trans. Commun. 36 (4) (1988) 465–470.

[23] Data Encryption Standard, Federal Information Processing Standard (FIPS), vol. 46, National Bureau of Standards, January 1977.

[24] C.S. Laih, L. Harn, C.C. Chang, Contemporary cryptography and its application, Flag, 2003.

[25] W. Diffie, M.E. Hellman, New direction in cryptography, IEEE Trans. Inform. Theory IT-22 (1976) 644–654.

[26] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (1978) 120–126.

[27] K.R. Castleman, Digital Image Processing, Prentice-Hall, New York, 1996.

[28] C.K. Chan, L.M. Po, Image vector quantization using Hadamard transform subspace, IEEE Region 10 Conference on Computer and Communication Systems, 1990, pp. 476–480.

About the Author—CHI-YUAN LIN received the B.S. degree in Electronic Engineering from National Taiwan University of Science and Technology in 1988, the M.S. degree in Electronic and Information Engineering from National Yunlin University of Science and Technology in 1998, and the Ph.D. degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 2004. Since 1983, he has been with the Department of Electronic Engineering at National Chi Yi Institute of Technology in Taiwan where he is now an associate professor. His research interests include image compression, neural networks, and information security.

About the Author—CHIN-HSING CHEN received the B.S. degree in Electrical Engineering from National Taiwan University, Taiwan, in 1980, and the M.S. and Ph.D. degrees in Electrical and Computer Engineering from the University of California at Santa Barbara, in 1983 and 1987, respectively. Since 1988, he has been with the Department of Electrical Engineering at National Cheng Kung University in Taiwan where he is now a professor. His current research interests include pattern recognition and image processing. He has published over 180 papers and given more than 80 technical presentations in public in more than 15 countries.