A NOVEL PERCEPTUAL IMAGE ENCRYPTION SCHEME USING GEOMETRIC OBJECTS BASED KERNEL

Prabhudev Jagadeesh[1], P. Nagabhushan[2], R. Pradeep Kumar[3]

[1]Department of Studies in Computer Science, University of Mysore, India
jagadish_prabhu@yahoo.com
[2]Department of Studies in Computer Science, University of Mysore, India
pnagabhushan@hotmail.com
[3]Amphisoft Technologies Private Limited, Coimbatore, India
rpk.ind@gmail.com

ABSTRACT

The wide use of digital images and videos in various applications warrant serious attention to the security and privacy issues today. Several encryption techniques have been proposed in recent years as feasible solutions to the protection of digital images and videos. In many applications, such as pay-per-view videos, pay-TV and video on demand, one of the required features is that the quality of the video data be degraded only partially by some encryption technique and the encrypted data must still be partially perceptible. This feature referred to as 'Perceptual encryption' is the encryption algorithm that degrades the quality of media content according to security or quality requirements. In this work we propose a simple yet efficient technique for realizing perceptual encryption using geometric objects as kernels based on which the pixels are permuted. Confusion aspect that is required is realized by inserting the kernel on the image and thereby performing transposition of pixels based on the kernel formed out of geometric objects. The various parameters of geometric objects, number of objects and the position of the objects/kernel in the image are used as the key for encryption and later on for decryption. Further a choice of quality of the image required i.e., different levels of degradation is provided by adjusting the above parameters of the objects/kernel. From the results obtained it is evident that the proposed method which is more apt for perceptual encryption can also be used effectively for full image encryption with acceptable level of security.

KEYWORDS

Image encryption, Video encryption, Perceptual encryption and PSNR.

1. INTRODUCTION

The diverse multimedia services need different security levels and usability requirements, some of which should be defined and evaluated with human vision ability. A typical example is perceptual encryption, in which only partial information is encrypted and the encrypted image/video gives a rough view of the high quality services that are available. This feature makes it possible for prospective users to access low-quality versions of the multimedia services before actually buying them. It is desirable that the quality degradation be constantly controlled. Figure.1 shows a pictorial view of perceptual encryption system [1]. Regarding perceptual encryption, since there does not exist a well-accepted objective measure of visual quality of digital images and videos, the control factor is generally chosen to represent an estimated measure of the degradation. Further the control factor selected for the encryption scheme may not have a linear

DOI : 10.5121/ijcsit.2013.5414

relationship with the visual quality degradation but a larger value always means a stronger degradation. When the control factor is maximum, the strongest visual quality degradation of the specific algorithm is reached, which does not necessarily imply that it is the strongest degradation among all perceptual encryption algorithms.

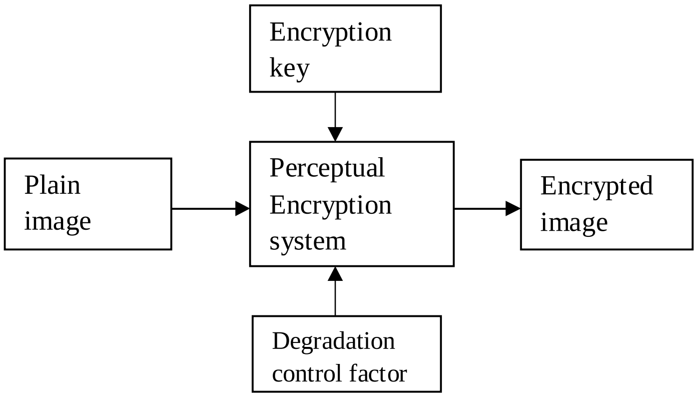


Figure 1. A typical perceptual encryption system

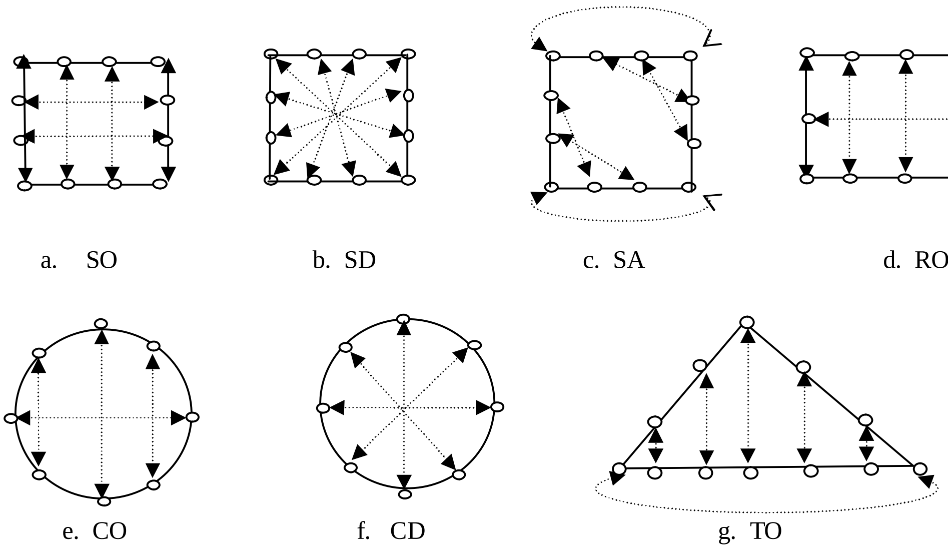
The rest of this paper is organized as follows. Section 2 presents the related work found in literature with regard to perceptual encryption. In Section 3, the proposed scheme for image scrambling based on geometric objects is discussed. Section 4 contains the experiments carried out and the results obtained. Section 5 presents the security analysis and quality of degradation of the proposed approach. Finally, Section 6 concludes the paper highlighting the research accomplishments and also proposing future directions.

2. RELATED WORK

In recent years, few perceptual encryption schemes have been proposed for images and videos [2-5]. In [6,14] perceptual encryption based on selectively encrypting some combination of bitplanes in the spatial domain and in the DCT or wavelet domain is proposed. Since different bitplanes have different significance for the quality of media content, the quality of encrypted images corresponding to different bitplanes being encrypted is tested. Generally, the encrypted image is unintelligible when at least seven bitplanes are encrypted. In [7] a perceptual image encryption scheme using iterative operation of local pixel shuffling and reversible histogram spreading is proposed in which image's local details are visually better encrypted compared to ordinary shuffling schemes. In [8], three variants to transparently encrypt JPEG2000 images are compared from a perceptual quality viewpoint. Here the focus is to predict the subjective quality of the encrypted images as given by the mean opinion score with available objective quality metrics. Furthermore, the objective quality measure that best suite an image quality for which a certain subjective quality is required is demonstrated. The selective encryption algorithms proposed in [9] is a special case of the perceptual encryption for images compressed with wavelet packet decomposition. In [10] the proposed technique performs the functions of encryption and watermarking simultaneously based on their respective key. The perceptual encryption scheme is based on AC component. The watermarking approach utilizes the DC component that is perceptually significant part, to embed the watermark. In [11], the encryption algorithm can be adjusted to produce cipher-image with varying perceptual distortion. Also the decryption algorithm is able to reconstruct the original image even if the encrypted image is JPEG compressed.

3. PROPOSED APPROACH

In the proposed work the security of the digital image is enforced employing the concept of perceptual security which refers to encrypted data's intelligibility. For data like image one need not completely encrypt the entire image but instead security can be provided if the image is made incomprehensible. The proposed work is a permutation based approach where the transpositions of pixels are guided by the kernel formed out of geometric objects. Basic geometric objects viz., Square, Rectangle, Circle and Triangle are used for transposition of pixels. The combination of various objects forms the kernel which defines the swapping pattern for the pixels. The pixels are shuffled according to the various objects and the swapping patterns defined for individual objects. The transposition of pixels as defined by the kernel results in a type of non-linear fashion of shuffling. The objects and the swapping patterns are listed in Figure. 2. The various objects and the swapping pattern make up the key for encryption and decryption. The position of the objects or the kernel is altered repeatedly as predefined to obtain the required level of degradation. During this process a pixel may undergo multiple swapping. For decryption the same algorithm is carried out, but now the shuffling of pixels is done considering the geometric objects in the reverse order. The overall design of the proposed technique is shown in Figure. 3.



a. SO b. SD c. SA d. RO

e. CO f. CD g. TO

Figure 2. Various Geometric objects and the swapping patterns.

SO - Square with opposite pixel swapping SD - Square with diagonal pixel swapping
SA - Square with adjacent pixel swapping RO - Rectangle with opposite pixel swapping
CO - Circle with opposite pixel swapping CD - Circle with diagonal pixel swapping
TO - Triangle with opposite pixel swapping

3.1 Algorithm

Step 1: Define various geometric objects as Abstract Data Types.

Step 2: Define the various swapping patterns for each object as operations that can be carried out on the different objects defined in ADT.

Step 3: Select the geometric objects to be used for scrambling the image from the set of objects defined in Figure.1 to form a kernel.

Step 4: For each object selected, define the various parameters namely *dimension*, *starting-position-point*, *swapping pattern*, *step-size-of-dimension*, *step-size-of- position-point* and the *number-of-iterations.*

Step 5: Form the *key* based on the objects selected and its various parameters.

Step 6: Place the object in the position as defined by the *starting-position-point* of the object in the key.

Step 7: Swap the pixels as defined by the swapping pattern in the *key*.

Step 8: Alter the dimension and position point of the object based on the *step-size-of-dimension* and *step-size-of position-point* respectively.

Step 9: Repeat step 7 and step 8 till the terminating condition based on *number-of-iterations* is reached.

Step 10: For each object in the kernel perform step 6 to 9.

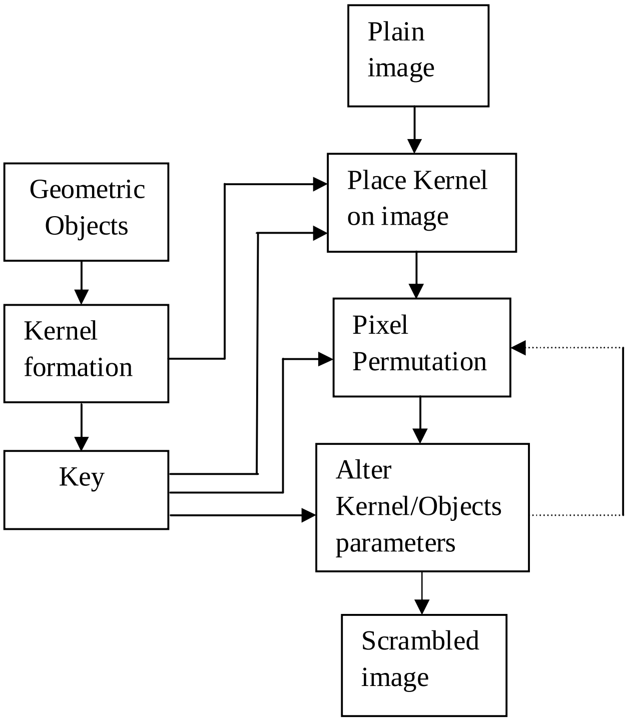


Figure 3. Proposed Perceptual Image Scrambling System

4. EXPERIMENTAL RESULTS

The proposed algorithm was tested on several standard images. The results obtained for images in Figure.4 are shown in Figure.5 – Figure.8. The results specify images with varied levels of perceptual quality, controlled by degradation level by varying the different parameters of the kernel.

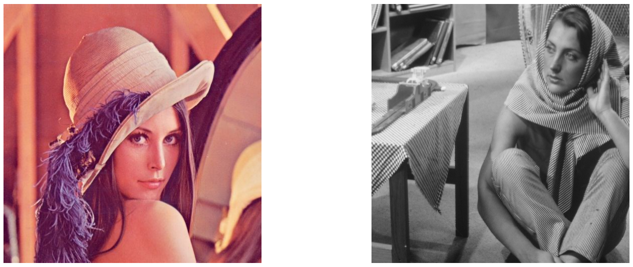
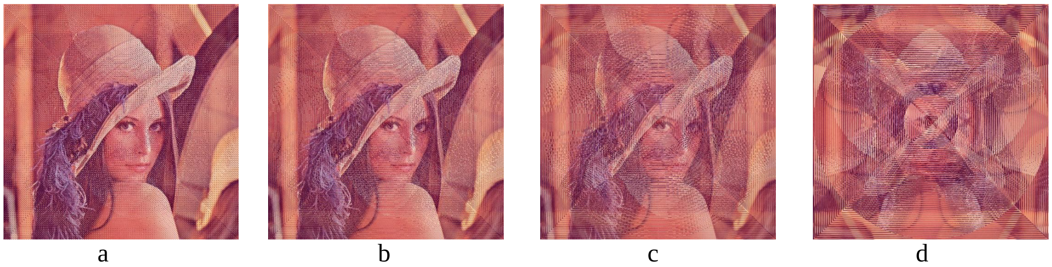


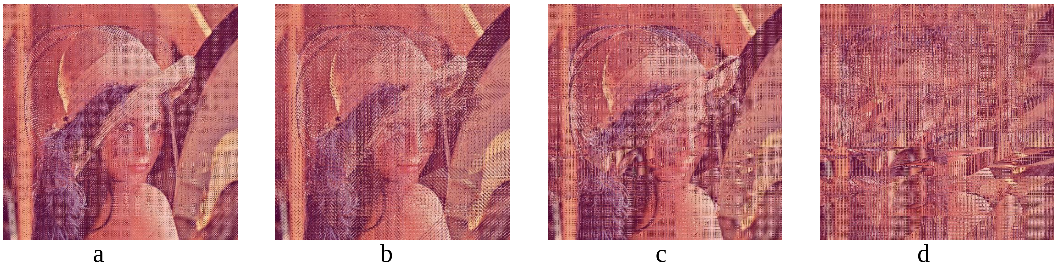
Image 1 Image 2

Figure 4. Plain-images



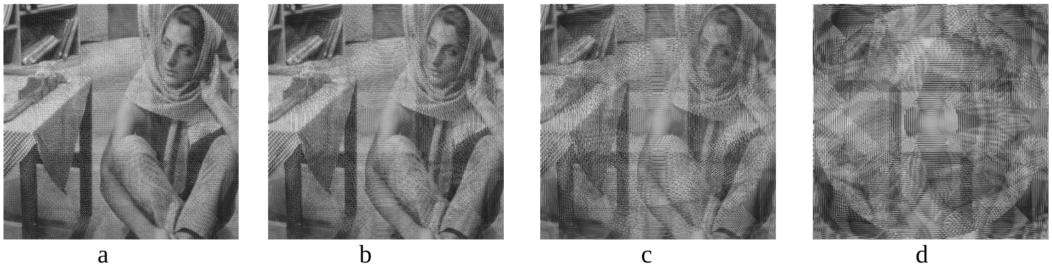
PSNR=16.667 PSNR=15.381 PSNR=13.720 PSNR=12.242

Figure 5. Perceptually Scrambled images with the kernel formed by objects (SO,CD)



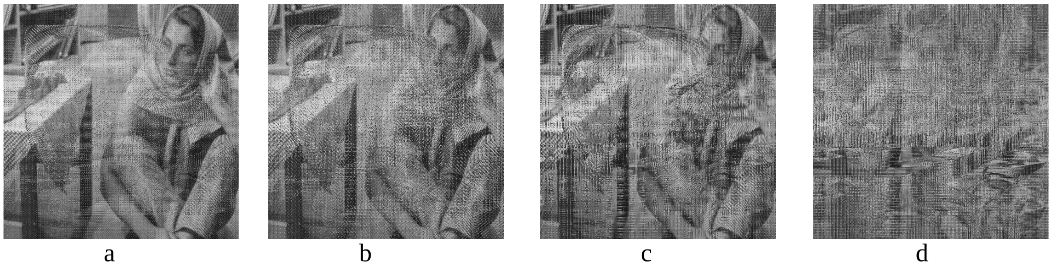
PSNR=15.835 PSNR=14.419 PSNR=14.162 PSNR=11.988

Figure 6. Perceptually Scrambled images with the kernel formed by objects (SO,RO,CD,TO)



PSNR=15.895 PSNR=14.626 PSNR=12.945 PSNR=11.536

Figure 7. Perceptually Scrambled images with the kernel formed by objects (CD,SO)



PSNR=15.205 PSNR=13.771 PSNR=13.471 PSNR=11.197

Figure 8. Perceptually Scrambled images with the kernel formed by objects (SO,CD,TO,RO)

5. Security Analysis of the proposed scheme

5.1 Perceptual Security

Since multimedia content has more redundancy than text or binary data, the encrypted data may still be somewhat comprehensible. Perceptual security which refer to the encrypted data's intelligibility can be measured both by subjective and objective metrics. In a subjective metric, scorers are asked to rate the scrambled data's quality level for various scrambled data of different quality. The typical quality levels for a subjective metric are 'completely understandable', 'partially understandable', and 'not understandable' [14]. 'Completely understandable' denotes that the scrambled image is completely understandable and even is of good quality. In this case, the encryption is considered to be not successful. 'Partially understandable' indicates that only a few parts of the scrambled image can be understood. For instance, only the shape is understandable, while the texture is uncertain. In this case, the scrambling is only suitable for applications not requiring high security. 'Not understandable' indicates that the scrambled image is completely incomprehensible which implies scrambling is successful in perceptual aspects.

An objective metric provides more efficient test methods and is suitable for computer based analysis. Naturally, the metric should be based on multimedia understanding techniques. As subjective assessments are expensive and time consuming, it is difficult to implement them onto a real time system. Objective assessments are automatic and mathematical defined. Subjective measurements can be used to corroborate the usefulness of objective measurements. Therefore objective methods have engrossed more attentions in recent years [12]. Thus, the quality metrics are more often used as the objective metric of encrypted data. The classic metric for audio quality is signal-to-noise ratio (SNR), and the one for image is peak signal-to-noise ratio (PSNR) [13]. In this work PSNR analysis is carried out to measure the quality of degradation and thereby the effectiveness of the proposed method. PSNR which is normally used to measure images' quality losses caused by operations such as compression, noising and transmission errors is computed by comparing the original image and the processed image.

Let $P=p_0\, p_1 \ldots p_{n-1}$ be the Plain-image and $C=c_0\, c_1 \ldots c_{n-1}$ be the Scrambled-image.
Also $(0 \le p_i\ , c_i \le L\text{-}1,\ i=0,1,\ldots,n\text{-}1)$

Scrambled-image's PSNR is computed as,

$$PSNR = 10\log_{10}\frac{L^2}{MSE},$$

where ,

$$MSE = \frac{1}{n}\sum_{i=0}^{n-1}(c_i - p_i)^2.$$

Here, *L* is the pixel's gray level. For an 8-bit image, *L*=256. Generally, the bigger PSNR is, higher is the scrambled-image's quality. Thus for a good image encryption algorithm, the PSNR of the scrambled-image should be small enough for concealing the content. As indicated in Figure.5 - Figure.8, smaller PSNR values obtained for higher degradation and larger PSNR values for lesser degradation corroborate the desired property of an efficient image encryption algorithm.

5.2 Correlation Analysis

Correlation coefficient can be used to measure the correlation between two pixels. An efficient image scrambling technique should strive to achieve lower correlation coefficient in scrambled image. To examine the correlation property of two horizontally adjacent pixels, two vertically adjacent pixels and also two diagonally adjacent pixels for the original image and scrambled image, 1000 pairs of adjacent pixels were selected randomly and the correlation coefficient of each pair is computed using Equations below:

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)).$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

Here x and y are grayscale values of two adjacent pixels in the image. Correlation coefficient values obtained for the perceptual scrambling of Image 1 and Image 2(Figure 6 and Figure 8) is shown in Table 1 as an instance. Higher value of correlation coefficient of original image indicates pixels in original image are highly correlated, whereas the smaller value of correlation coefficient of scrambled images indicate lesser correlation between image pixels which is the property desired from any image scrambling technique. Further the decrease in values of correlation coefficient as the degradation is increased corroborates the PSNR values obtained earlier.

Table 1. Correlation Coefficient of Original Image and Scrambled Images

Correlation Coefficient	Image 1					Image 2				
	Original image	Scrambled images				Original image	Scrambled images			
		a	b	c	d		a	b	c	d
Horizontal	0.9844	0.4513	0.2464	0.2050	0.0459	0.9455	0.4555	0.2507	0.1951	0.0602
Vertical	0.9752	0.4417	0.2396	0.1606	-0.0261	0.9643	0.4890	0.2780	0.2220	0.0702
Diagonal	0.9685	0.3770	0.2391	0.1582	-0.0146	0.9828	0.4612	0.2500	0.1859	-0.0223

6. CONCLUSION

In the proposed work the confidentiality of digital image is enforced by employing the concept of perceptual security. Instead of complete encryption of image, the image is only partially scrambled to bring in the required quality of degradation. Pixel permutation is supervised by the kernel formed by various geometric objects. The combination of various geometric objects and several options of swapping patterns provides a kind of non-linear permutation of pixels. The objective analysis carried out by measuring the peak signal to noise ratio between original image and scrambled image indicates that scrambling is successful with regard to perceptual aspect. The results obtained indicates, though the proposed method suite perceptual encryption of images, the same algorithm when employed with more complex kernels, acts as an efficient image scrambling scheme. As an enhancement, instead of pixel-permutation, image-block permutation can be employed as this would further reduce the computational complexity. Thus, the proposed technique can be used either for lightweight encryption in which the scrambled image has a degraded visual quality but reveals the contents of the original image, or for strong encryption in which the scrambled image does not reveal any information about the original image.

REFERENCES

[1] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, (2007), “On the design of perceptual MPEG-Video encryption algorithms”, IEEE Transactions on Circuits and Systems for Video Technology, pp 214–223.

[2] Parameshachari B D, K M Sunjiv Soyjaudah, Chaitanyakumar M V, (2013), “A Study on Different Techniques for Security of an Image”, International Journal of Recent Technology and Engineering (IJRTE), Volume-1, Issue-6.

[3] A. Torrubia and F. Mora, “Perceptual cryptography on MPEG layer III bit-streams”, (2002), IEEE Trans. Consumer Eletronics, vol. 48, no. 4, pp.1046–1050.

[4] S. Lian, J. Sun, and Z. Wang, (2004), “Perceptual cryptography on SPIHT compressed images or videos”, IEEE International Conference on Multimedia and Expro (I) , Vol. 3, pp 2195–2198.

[5] Potdar, U, Talele, K.T, Gandhe, S.T, (2010), “Perceptual video encryption for multimedia applications”, Second International Conference on Computer Engineering and Applications.

[6] Khan, Jeoti, Khan, M,A, (2010), “Perceptual encryption of JPEG compressed images using DCT coefficients and splitting of DC coefficients into bitplanes”, International Conference on Intelligent and Advanced Systems.

[7] Bian Yang, Busch, C, XiaMu Niu, (2009), “Perceptual image encryption via reversible histogram spreading”, Proceedings of 6th International Symposium on Image and Signal Processing and Analysis, 2009.

[8] A. Torrubia, and F. Mora, (2003), “Perceptual cryptography of JPEG compressed images on the JFIF bit-stream domain”, IEEE International Symposium on Consumer Electronics, ISCE.

[9] S. Lian, X. Wang, J. Sun, and Z. Wang, (2004), “ Perceptual cryptography on wavelet transform encoded videos”, International Symposium on Intelligent Multimedia, Video and Speech Processing.

[10] Khan, M.I., Jeoti, V., Malik, A.S, (2010), “Designing a joint perceptual encryption and blind watermarking scheme compliant with JPEG compression standard”, International Conference on Computer Applications and Industrial Electronics , pp 688-691.

[11] Ahmed, F., Siyal, M.Y. ; Abbas, V.U, (2010), “A Perceptually Scalable and JPEG Compression Tolerant Image Encryption Scheme”, Fourth Pacific-Rim Symposium on Image and Video Technology.

[12] Parameshachari B D, K M Sunjiv Soyjaudah, Sumithra Devi K A, (2013), “Image Quality Assessment for Partial Encryption Using Modified Cyclic Bit Manipulation”, International Journal of Innovative Technology and Exploring Engineering .

[13] Siu-Kei Au Yeung, Shuyuan Zhu, Bing Zeng, (2010), “Quality assessment for a perceptual video encryption system”, IEEE International Conference on Wireless Communications, Networking and Information Security.

[14] Shiguo Lian, (2008), Multimedia Content Encryption – Techniques and Applications, CRC Press.

[15] W. Zeng, H. Yu, and C.-Y. Lin, Eds, (2006), Multimedia Security Technologies for Digital Rights Management, Academic Press, Inc.

[16] Furht , Kirovsk, (2005), Multimedia Security Handbook, CRC Press.

Authors

Prabhudev Jagadeesh, is currently pursuing PhD at University of Mysore, India. He completed his B.E degree in Computer Science and Engineering in 1997 from University of Mysore and M.Tech degree in Software Engineering in 2001 from VTU, Belgaum, India. He has over 15 years of teaching and research experience. His areas of research include Computer Vision and Information Security.

Dr. P Nagabhushan (BE-1980, M.Tech.1983, PhD-1989) is presently Professor, Department of Studies in Computer Science and also Chief Nodal Officer, Credit based choice based Education, University of Mysore, Mysore. He is an active Researcher in the areas pertaining to Pattern Recognition, Document Image Processing, Symbolic Data Analysis and Data Mining. Till now he has successfully supervised 22 PhD candidates. He has over 400 publications in journals and conferences of International repute. He has chaired several international conferences. He is a visiting professor to USA, Japan and France. He is a fellow of Institution of Engineers (FIE) and Institution of Electronics and Telecommunication Engineers (FIETE) India.

Dr. R.Pradeep Kumar is CEO of Amphisoft Technologies Private Ltd., Coimbatore, India. He holds PhD in Computer Science from University of Mysore. His areas of research include Image Processing, Video Analytics, Symbolic data, Knowledge Engineering. He is currently supervising 7 PhD candidates under Anna University. He has served as Head of Training and R&D sections at TCS Chennai. He has more than 25 publications in his areas of research.