A REVIEW OF ROBUST HASHING METHODS FOR CONTENT BASED IMAGE AUTHENTICATION

By

LOKANADHAM NAIDU VADLAMUDI * RAMA PRASAD V. VADDELLA ** VASUMATHI DEVARA ***

* Assistant Professor, Department of Information Technology, Sree Vidyanikethan Engineering College, Andhra Pradesh, India.
** Professor, Department of Computer Science and Engineering, Sree Vidyanikethan Engineering College, Andhra Pradesh, India.
*** Professor, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Telangana, India.

ABSTRACT

At present, the multimedia data will be transmitted rapidly using an internet. But, whether the data reaches the recipient without tampering is questionable. The current multimedia editing software allows adversaries to alter multimedia data without changing its visual perception. Different categories of approaches exist for verifying the integrity as well as authenticity of multimedia data. The Content Based Authentication (CBA) is one among them. This review paper describes various Content Based Image Authentication (CBIA) methods, which have been developed for integrity verification of images. And also, this paper summarizes various techniques used in existing image authentication methods to extract robust features. In addition, this paper discusses the important characteristics of a CBIA approach, limitations of existing methods and future research directions. The development of robust and secure image authentication method for content authentication is still an open challenge for current researchers.

Keywords: Content Based Image Authentication, Image Hashing, Integrity Verification, Robustness, Fragility.

INTRODUCTION

With the modern advancements in multimedia technologies, the verification of integrity of multimedia content like text, images, audio, video, etc., is a challenging task. The multimedia content is distributed through an insecure internet medium that causes vulnerability. In internet, there is a chance for the opponent to modify or tamper the multimedia content during transmission. Due to that, providing integrity to multimedia content is a challenging task in digital communication. For checking the integrity of multimedia content, different integrity verification methods have been developed. It [17], [18] includes, 1) Watermarking methods which embed a text or images into a multimedia content. Later, the embedded data are extracted for integrity verification, and 2) Digital Hashing methods use various existing conventional cryptographic algorithms [4], [11], [14], [18] including Message Digest, Secure Hash Authentication, etc., for generating a digital hash. The obtained hash is used in integrity verification process. The main problem with these cryptographic algorithms is that, they are very sensitive to the change in multimedia content and also require more time to process multimedia content [11], [17] due to the large size. Conventional crypto hash methods are not suitable to check the integrity multimedia content. The alternative method to verify multimedia content is Content Based Authentication.

1. Objective

- To present various existing content based image authentication methods.
- To provide insights of techniques used in existing methods to extract robust features from images.
- To discuss various performance requirements needed to develop efficient image authentication methods.

2. Content Based Image Authentication

Content Based Image Authentication [1], [11], [18] is an efficient and semi-fragile approach used to verify a query image is a copy of original image or tampered version.

The general framework of the Content Based Image Authentication is shown in Figure 1.

To verify the authenticity of images using CBIA approach, human perceptual features like edges, colour, textures or salient content, etc., are extracted from digital images. The secure binary hash will be generated from extracted features using a secret key is shown in Figure 1(a). The obtained hash is used in the authentication process to verify the integrity as well as authenticity of the images. The hash will be transmitted to the recipient by appending or embedding it into an original digital image. The recipient produces the hash of the received image using the same hash generation procedure used as a source. The both hashes are compared to make the query image as an authentic or fabricated version is shown in Figure 1(b).

The main goal of CBIA approach is to extract robust features from digital images. The extracted robust features must be sensitive to Content Changing Manipulations (CCM) and must tolerate insignificant Content Preserving Manipulations (CPM) [11], [18]. Content Changing Manipulations change the image content as well as perceptual meaning of the image. Some of the Content Changing Manipulations are: 1) Removing image objects, 2) Moving of image objects or changing their positions, 3) Adding new objects, and 4) Changing image characteristics like colour, texture, structure and impression. Content Preserving Manipulations made small change in value of image pixels that result in different levels of visual distortion, no changes in image content and carries the same perceptual meaning. The various Content Preserving Manipulations include, image rotation, cropping, scaling, adding noise, compression, transmission errors, colour conversions, contrast adjustment, changes in brightness, etc., or incidental distortion due to transmission errors. And also, the Content Image Authentication approach must satisfy the following properties [5], [11].

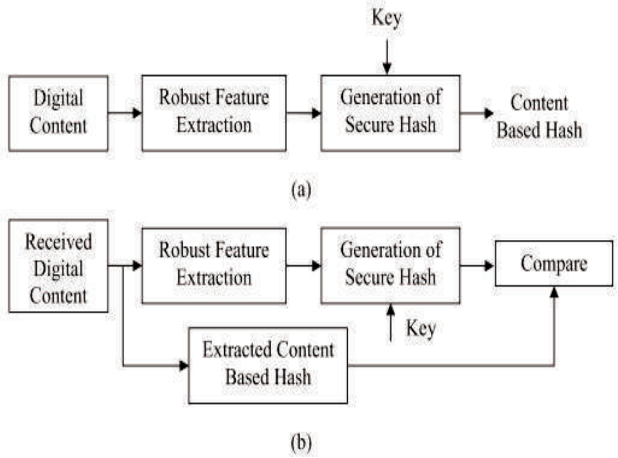
Key
Digital Content
Robust Feature Extraction
Generation of Secure Hash
Content Based Hash
(a)
Received Digital Content
Robust Feature Extraction
Generation of Secure Hash
Compare
Key
Extracted Content Based Hash
(b)

Figure 1. General Framework of Content Based Image Authentication, (a) Hash Generation Process and, (b) Hash Verification Process

- Robustness: The robustness property says that, the image hash should be invariant to CPM and sensitive to CCM.
- Fragility: The fragility property describes that, for visually distinct images, the authentication method should produce different hashes.
- Key dependent: It tells that, for two different secure keys, the hash method must generate different hashes for a single image.
- Security: It says that, without knowing the details of a secret key, the hash will not be known or tampered.

3. Literature Review

Yong Soo Choi and Jong Hyuk Park [1] proposed an image authentication method, GLOCAL using hierarchical histogram bin population. Shijun Xiang and Hyoung Joong Kim [4] and Shijun Xiang, et al., [20] designed image hashing methods for content authentication using statistical features like image histogram and mean. The methods [1], [4], [20] perform spitting or merging operation on histogram bins for generating wider bins. The image hash has generated by comparing the pixel count of neighbouring bins. The advantage of method [1] is that, it will produce a short length hash for wider bins. The hash obtained from the histogram of the image is more robust to Content Preserving Manipulations as well as incidental distortion. The drawbacks of histogram methods are, 1) They are not robust to Content Changing Manipulations and 2) Images can be easily tampered without changing the shape of the histogram. Nighat Jamil and Arshad Aziz [10], and Fawad Ahmed, et al., [12] proposed a robust and secure image hashing scheme based on Discrete

Wavelet Transform (DWT). The method [12] divides an image of size 256×256 pixels into non-overlapped equal blocks of size 16×16 pixels. The hash of the image is generated from sub-band coefficients which are generated by decomposing the image using 2D Discrete Wavelet Transform. S. M Saad [17] developed a modified Structural Digital Signature (SDS) algorithm based on DWT and secret filter parameterization. In this method, the key dependant parametric wavelet filters are incorporated in DWT domain to improve the security against malicious attacks. The secure hash is generated from parent-child pairs of sub-band coefficients. Yang Ou, Chul Sur, and Kyung Hyune Rhee [13] proposed a discriminative image hashing scheme based on Region of Interest (ROI). They have combined global and local features of the image to produce the discriminative hash which is robust to CPM and sensitive to CCM. They have used Harris corner detector for selecting ROI points from 2D DWT LL sub-band of the image. The Global and local features are extracted by applying the Fourier-Mellin Transform (FMT).

Rui Sun and Wenjun Zeng [2] developed FMCS image hash algorithm based on Compressive Sensing (CS) and Fourier-Mellin Transform (FMT) techniques. They used Fourier-Mellin transform to improve the performance of image hash on rotation, scaling and translation distortions. The Fourier Transform is applied to the image to get coefficients which are invariant to translation. This method has been implemented with different random projections to produce a secure image process. Li Weng and Bart Preneel [5] proposed a block based perceptual image hash method for image content verification. This method uses uncorrelated, low frequency phase coefficients of Discrete Fourier Transform (DFT) in an image hash generation. Swaminathan, et al. [19] designed, a robust and secure image hashing method based on Fourier Mellin Transformation. This method is invariant to affine transformations. For generating a secure and robust hash method, they have incorporated key dependent randomization process.

Zhenjun Tang, et al. [8] proposed a Lexicographical framework to generate image hash using Discrete Cosine Transform (DCT) and Non-negative Matrix Factorization (NMF) approaches. This method mainly consists of two parts: 1) Dictionary construction and 2) Hash generation. The dictionary contains a collection of feature vectors called words which represent the various characteristics of image blocks. In hash generation process, 2D DCT is applied on image block to capture the structure of the image block. The structural similarity metric is used to select the most similar features from the dictionary. The selected features are combined to produce an intermediate hash. The final hash is produced from an intermediate hash. Young-Dong Zhang, et al., [23] proposed a secure image hashing method based on Hotelling's T-square Statistic (HTS) and Principal Component Analysis of DCT coefficients. This method transforms the image into 8×8 block of DCT coefficients and then DC and AC coefficients from each block are extracted. The extracted coefficients are encrypted using the choatic sequence. The Eigen vector is computed from encrypted coefficients using Singular Vector Decomposition (SVD). The HTS values are calculated as an Eigenvector. Later, HTS values are quantized to produce the final digital signature for the input image.

Guangjie Liu, et al. [3] developed image authentication method based on image moments which are invariant to image translations, i.e., even an image is rotated or scaled, the centralized moments are not changed. The [3] method uses Hu-invariant moments as features in the hash construction process which are robust against various distortions like rotation, blurring, noise addition and JPEG compression. Seven Hu-invariant moments are constructed from the second and third order normalized moments. These moments are used to verify the integrity and authenticity of the images. Yanqiang Lei, et al. [6] developed image authentication method based on Radon Transform. It is an efficient method for analyzing the 1D and 2D signals in the spatial domain as well as projection space. It will project the image along a radial line at a specific angle to obtain radon components. The radon components are invariant to image rotation, scaling, and translation. The DFT is applied on constructing moments from radon components, then, the DFT coefficients are quantized to get the final hash.

Zhihua Xu, et al. [7] proposed a novel image copy detection scheme based on Scale Invariant Feature Transform (SIFT) and Multi-resolution Histogram Descriptor (MHD). SIFT detector extracts features from input image which are invariant to rotation, scaling, translation and significant illumination changes. A set of robust, homogenous and large size circular patches are constructed using the SIFT detector. Later, the MHD is applied to generate a feature vector for each circular patch. The final hash is produced by sampling and normalizing the feature vector. Lina Wang, et al., [9] designed an image authentication method using a Gabor filter. In this method, three reference metrics are used to obtain the robust hash. They are reference scale, reference direction, and reference block. The reference scale is computed to make the hash invariant to scaling. To make the hash invariant to rotation, the reference direction is calculated. To make the hash invariant to shifting or cropping, the third metric reference block is computed. The final hash is constructed using path selection strategy by connecting various image blocks.

Marco Tagliasacchi, et al. [15] proposed an image hashing algorithm based on Compressive Sensing and Wyner-Ziv coding principles. This method divides an input image into blocks of size 16×16 pixels. For every block, the vector of average of luminance components is computed. Different linear random projections are applied on components with a random seed. The hash is generated by quantizing the random projections through the Uniform scalar quantizer. The hash has strong computational security against different malicious attacks. Han-ling Zhang, et al., [16] designed an image authentication scheme based on the DWT, Radon Transform, Log Mapping and Fourier Transform techniques. Level-2, 2D DWT is performed on the input image. The radon transform is performed on the coefficients of an LL sub-band of level-2 2D DWT at a specified angle. The invariant features are obtained by applying the Log mapping and further Fourier transform is applied to get robust features. Later, features are quantized and then gray code is applied on quantized features to generate a hash.

Vishal Monga and M. Kivac Mihcak [21] proposed a Non-negitive Matrix Factorization (NMF) method for robust and secure image hashing. It has two important properties like additivity and minimizing error capability. The additivity property captures the local components of the image, which can significantly reduce misclassification. Kai Chen, Xinglei Zhu, and Zhishou Zhang [22] proposed a hybrid content based image authentication scheme which integrates two methods like 1) Robust content-based authentication and 2) Semi-fragile crypto-hash based authentication. Content-Based Authentication uses Random Blocks Mapping (RBM) process to perform on input image and covert it into small blocks. Crypto-Based Authentication method divides the image into non-overlapping 8×8 blocks. DCT coefficients are computed for each block and then quantization is applied on DCT coefficients to generate the image hash.

4. Image Content Verification Process

To verify the image content and measure the similarity between the original and the manipulated images, a metric called Normalized Hamming Distance (NHD) is used. The NHD is measured between two hashes of the original and query images. It is defined as:

$$\text{NHD}\,(\text{hash}_1,\ \text{hash}_2) = \frac{1}{N}\sum_{n=1}^{N}\left|hash_1(n) - hash_2(n)\right| \qquad (1)$$

The hamming distance is very close to 0.5 or above in case of malicious modifications as well as dissimilar images. In case of legitimate modifications or for visually similar images, the hamming distance is close to zero. Most of the methods, except [3], [6], [15], [17], [23] reported in this survey paper incorporated the Normalized Hamming Distance (NHD) metric for verifying the image content and identifying the malicious modifications on images.

5. Performance Analysis and Discussions

The performance of any image hash method depends on the following parameters. They are: 1) Robust image features used in hash generation, 2) Robustness, 3) Fragility, 4) Computational complexity, and 5) Size of the hash. The important stage of any hash method is that, the extraction of image features. Robust image features will play a major role in the generation of efficient hash. The selected image features used in hash generation process must allow insignificant modifications and should identify malicious modifications on images. The methods discussed in this review paper extracted various image features. The method and the type of image feature used in hash generation process listed in Table 1. Table 1 presents various feature extraction techniques, image size as well as block size utilized for feature extraction in existing methods.

The hash method should not only extracts robust features, but also produce a secure hash. The security of the image hash depends on hash generation algorithm. For generating a secure hash, the hash method must incorporate various random permutation procedures in hash generation process. The permutation procedures generate permutation sequences using a secret key. In order to generate a secure image hash, the image pixels are permuted before feature extraction or features are permuted after extraction. The methods [10], [12], [22] uses permutation sequences for generating a secure hash. The method [5] uses Pseudo Random Number Generator (PRNG) in hash generation process for making a secure hash. The hash method must also support good robustness property i.e., for which it is sensitive and insensitive to various attacks. A good hash method should identify the tamper locations on the images when malicious modifications are performed. Most of the existing methods are experimented to estimate the robustness on various Content Preserving manipulations. The methods [3], [5], [9], [15], [17], [19], [23] are experimented to check the robustness on both Content Preserving and Content Changing attacks. The methods [1], [2], [4], [6], [8], [10] are not tested for robustness against Content Changing manipulations. Table 2 shows the set of Content Preserving attacks experimented for testing the robustness. The other factor that influences the performance of the image hashing method is fragility or anti-collision also, the performance of the hash method depends on computational complexity. Digital images are very large in size and require more time to process. The hash method must reduce the time to compute robust and secure hash. The existing methods use either entire image or image block as a basic unit in hash

Method	Technique used	Features Extracted	Image size (Pixels)	Block size (Pixels)
[1]	Hierarchical Histogram	Histogram bin population	-	-
[2]	Compressive Sensing and Fourier Mellin Transform	Random Projections	256×256	8×8
[3]	Hu-Moments	Invariant Hu-moments	400×400	16×16
[4]	Image Histogram	Histogram bin population	256×256	-
[5]	Discrete Fourier Transform (DFT)	Low frequency coefficients	512×512	64×64
[6]	Radon Transform and DFT	Image movements	256×256	-
[7]	Scale Invariant Feature Transform (SIFT) and Multi-resolution Histogram Descriptor (MHD)	Local invariance patches	512×512	-
[8]	DCT and Non-Negative Matrix Factorization (NMF)	DCT coefficients	512×512	64×64
[9]	Gabor Filter	Reference scale, direction, block	256×256	-
[10]	Discrete Wavelet Transform (DWT)	DWT coefficients	256×256	16×16
[12]	Random Pixel Modulation and DWT	DWT coefficients	256×256	16×16
[13]	DWT and Fourier Mellin Transform	DWT global and ROI local features	-	16×16
[14]	Discrete Cosine Transform (DCT)	NMF coefficients	512×512	32×32
[15]	Compressive Sensing and Wyner-Ziv	Luminance components	512×512	16×16
[16]	DWT, Radon Transform, Log Mapping and DFT	Invariant features from log mapping	256×256	-
[17]	DWT with secret parameterization	DWT parent child pairs	-	-
[20]	Image Histogram	Histogram bin population	512×512	-
[21]	Non-negative Matrix Factorization	NMF coefficients	-	-
[22]	Discrete Cosine Transform (DCT)	Edges, DCT coefficients	-	64×64
[23]	Hotelling's T-Square Statistic (HTS), DCT	DCT AC, DC coefficients	512×512	8×8

Table 1. List of Techniques used in Existing Image Authentication Methods to Extract Robust Image Features

Method	Rotation	Scaling	Cropping	Adding Noise	Filtering	JPEG Comp -ression	Blurring
[1]	×		×	×	×	×	
[2]	×	×			×		
[3]	×			×		×	×
[4]	×	×	×	×	×	×	
[5]		×		×		×	
[6]	×	×	×	×	×		
[7]			×		×		×
[8]		×		×	×	×	×
[9]	×	×	×	×		×	
[12]	×		×			×	
[13]		×	×	×			×
[14]		×				×	
[15]				×		×	
[16]	×	×		×	×	×	
[17]	×	×					
[19]	×	×	×	×	×	×	
[20]	×	×	×	×	×	×	
[21]	×	×					
[22]			×	×		×	
[23]				×		×	

Table 2. List of Content Preserving Attacks used in Existing Methods to Estimate the Robustness

generation process. The main advantage of the block based methods is to identify tamper locations easily, but it produces larger hash in size [5]. The size of the image block also influence the performance of the hash method. The final parameter that influence the performance of the hash method is hash size. The hash method must produce short length hash, which improves the performance and requires less bandwidth for transmitting the hash to the recipient.

Conclusions and Future Research Directions

Content Based Image Authentication, is an efficient approach used to verify the query image as an original copy or a fabricated version. In this paper, the authors have presented an in-depth study of existing image authentication methods. The existing methods utilized various feature extraction techniques in order to extract robust features for generating a secure image hash. The limitations of the existing authentication methods include: 1) The image features used in hash construction are not robust to both content changing as well as content preserving manipulations, 2) The existing hash methods are not incorporated into the security mechanisms for producing a secure hash, and 3) No method fulfills all the requirements of Content Based Image Authentication approach, i.e., existing methods are lacking either in security aspects or robustness capabilities. The feature research directions towards the development of efficient image authentication methods are: 1) Image feature set randomization to prevent various cryptographic attacks, 2) Extraction of robust features to identify malicious attacks and invariant to common image processing operations like geometric distortions, additive noise, filtering, etc., and 3) Design and development of robust image hashing methods for authenticity verification as well as retrieval of visually similar images from large databases.

References

[1]. **Yong Soo Choi and Jong Hyuk Park, (2012).** "Image Hash Generation Method using Hierarchical Histogram". *Journal of Multimedia Tools and Applications,* Vol. 61, No. 1, pp. 181-194.

[2]. **Rui Sun and Wenjun Zeng, (2012).** "Secure and Robust Image Hashing via Compressive Sensing". *Journal of Multimedia Tools and Applications,* Vol. 70, No. 3, pp. 1-15.

[3]. **Guangjie Liu, et al. (2011).** "A Passive Image Authentication Scheme for Detecting Region Duplication Forgery with Rotation". *Journal of Network and Computer Applications,* Vol. 34, No. 5, pp. 1557-1565.

[4]. **Shijun Xiang and Hyoung Joong Kim, (2011).** "Histogram Based Image Hashing for Searching Content-Preserving Copies". *Transactions on Data Hiding Multimedia Security VI,* Vol. 6730, pp. 83-108.

[5]. **Li Weng and Bart Preneel, (2011).** "A Secure Perceptual Hash Algorithm for Image Content Authentication". *Communications and Multimedia Security,* Vol. 7025, pp. 108-121.

[6]. **Yanqiang Lei, Yuangen Wang, and Jiwu Huang, (2011).** "Robust Image Hash in Radon Transform domain for Authentication". *Journal of Signal Processing: Image Communication,* Vol. 26, No. 6, pp. 280-288.

[7]. **Zhihua Xu, et al. (2011).** "A Novel Image Copy Detection Scheme Based on the Local Multi-resolution Histogram Descriptor". *Journal of Multimedia Tools and Applications,* Vol. 52, No. 2-3, pp. 445-463.

[8]. **Zhenjun Tang, et al. (2011).** "Lexicographical Framework for Image Hashing with Implementation based on DCT and NMF". *Journal of Multimedia Tools and Applications,* Vol. 52, No. 2-3, pp. 325-345.

[9]. **Lina Wang, et al. (2011).** "Image Authentication based on Perceptual Hash using Gabor Filters". *Journal of Soft Computing,* Vol. 15, No. 3, pp. 493-504.

[10]. **Nighat Jamil and Arshad Aziz, (2010).** "A Unified Approach to Secure and Robust Hashing Scheme for Image and Video Authentication". In *Proc. of 3rd Int. Congress on Image and Signal Processing (CISP-2010),* pp. 274-278.

[11]. **Shui-Hua Han and Chao-Hsien Chu, (2010).** "Content-based Image Authentication: Current Status, Issues and Challenges". *International Journal of Information Security,* Vol. 9, No. 1, pp. 19-32.

[12]. **Fawad Ahmed, M.Y. Siyal, and Vali Uddin Abbas, (2010).** "A Secure and Robust Hash-Based Scheme for Image Authentication". *Journal of Signal Processing,* Vol.90, No. 5, pp. 1456-1470.

[13]. **Yang Ou, Chul Sur, and Kyung Hyune Rhee, (2010).** "Discriminative Image Hashing Based on Region of Interest". In *Proc. of 16 Int. Conf. on Advances in Multimedia Modeling,* Vol. 5916, pp 701-706.

[14]. **Ammar M. Hassan, et al. (2009).** "Semi Fragile Image Authentication using Robust Image Hashing with Localization". In *Proc. of Second International Conf. on Machine Vision (ICMV-09),* pp. 133-137.

[15]. **Marco Tagliasacchi, et al. (2009).** "Hash-Based Identification of Spare Image Tampering". *IEEE Trans. on Image Processing,* Vol. 18, No. 11, pp. 2491-2504.

[16]. **Han-Ling Zhang, et al. (2009).** "Content Based Image Hashing Robust to Geometric Transformation". In *Proc. of Second Int. Symposium on Electronic Commerce and Security (ISECS-09),* pp. 105-108.

[17]. **S.M. Saad, (2009).** "Design of a Robust and Secure Digital Signature Scheme for Image Authentication over Wireless Channels". *IET Information Security,* Vol. 3, No. 1, pp. 1-8.

[18]. **Adil Haouzia and Rita Noumeir, (2008).** "Methods for image authentication: A Survey". *Journal of Multimedia Tools Applications,* Vol. 39, No. 1, pp. 1-46.

[19]. **Swinathan Ashwin, et at. (2006).** "Robust and Secure Image Hashing". *IEEE Trans on Inf. Forensics and Security,* Vol.1, No. 2, pp. 215-230.

[20]. **Shijun Xiang, et al. (2007).** "Histogram based Image Hashing Scheme Robust against Geometric Deformations". In *Proc. of 9th International Workshop on Multimedia and Security (MMS-07),* pp. 121-128.

[21]. **Vishal Monga and M. Kivac Mihcak, (2007).** "Robust and Secure Image Hashing via Non–Negative Matrix Factorizations". *IEEE Transaction on Information Forensics and Security,* Vol. 2, No. 3, pp. 376-390.

[22]. **Kai Chen, Xingleizhu, and Zhishou Zhang, (2007).** "A Hybrid Content-Based Image Authentication Scheme". In *Proc. of Advances in Multimedia Information Processing (PCM-2007),* Vol. 4810, pp. 226-235.

[23]. **Young-Dong Zhang, et al. (2007).** "Secure and Incidental Distortion Tolerant Digital Signature for Image Authentication". *Journal of Computer Science and Technology,* Vol. 22, No. 4, pp. 523-526.

ABOUT THE AUTHORS

Lokandham Naidu Vadlamudi is currently working as an Assistant Professor in the Department of Information Technology at Sree Vidyanikethan Engineering College, Tirupati, India. He received his B.Tech Degree from the JNT University, Hyderabad and the M.E. degree in Computer Science and Engineering from Sathyabama University, Chennai. He is also a Research Scholar at JNT University, Hyderabad, India. He has published a Research Paper in an International Journal and presented a paper in an International Conference. His areas of research interests include Image Processing and Information Security. He is a life member of ISTE and IAENG.

Dr. Rama Prasad V. Vaddella is presently working as a Professor in the Department of Computer Science and Engineering at Sree Vidyanikethan Engineering College, Tirupati, India. He received his M.Sc (Tech.) Degree in Electronic Instrumentation from Sri Venkateswara University, Tirupati, India and M.E Degree in Information Systems from BITS, Pilani, India. He has worked as an Assistant Lecturer in BITS, Pilani, Lecturer in Computer Science and Engineering, Associate Professor in RVR and JC College of Engineering, Guntur, India and worked as Professor and Head of Information Technology Department at Sree Vidyanikethan Engineering College, Tirupati, India. He was awarded the Ph.D. Degree in Computer Science by J.N.T. University, Hyderabad, for the thesis in Fractal Image Compression. He has also worked as a Research Assistant at Indian Institute of Science, Bangalore, India. He has published about 20 papers in National and International Journals and presented several papers in National and International Conferences. He is also a reviewer for 10 International Journals. His current areas of research interest include Computer Graphics, Image Processing, Computer Networks, Computer Architecture, and Neural Networks. He is a member of IEEE, IACSIT, IAENG, ISTE and CSI.

Dr. Vasumathi Devara is presently working as a Professor in the Department of Computer Science and Engineering at JNTU College of Engineering, Hyderabad, India. She received her B.Tech Degree from JNT University, Hyderabad and received M. Tech and Ph.D. Degrees in Computer Science and Engineering from JNT University, Hyderabad, India. She has 15 years of teaching experience. Currently, she is guiding 10 Ph.D scholars. She has 20 International publications and presented 22 research papers in National and International Conferences. Her research areas of interest are Data Mining, Image Processing, and Data Mining. She is a life member of ISTE and IE.