Implementation of Technique for Image Authentication using Regular LDPC Codes

Imran Ali Khan
All Saints' College of Technology, Bhopal

Bhanu Pratap Singh Sengar
All Saints' College of Technology, Bhopal

ABSTRACT

In this paper, we propose an approach using encryption technique and LDPC source coding for the image authentication problem. Image authentication is important in content delivery via untrusted intermediaries, such as peer-to-peer (P2P) file sharing. Many differently encoded versions of the original image might exist. In addition, intermediaries might tamper with the contents. Distinguishing legitimate diversity from malicious manipulations is the challenge addressed in this research.

The key idea is to provide a Slepian-Wolf encoded quantized image projection as authentication data which is again encrypted using a secret key cryptography before ready to send. This can be correctly decoded with the help of an authentic image as side information. This mechanism provides the desired robustness against legitimate variations while detecting illegitimate modification. The decoder incorporating expectation maximization (EM) algorithms can authenticate images which have undergone contrast, brightness and even warping adjustments. Our novel authentication system also others tampering localization by using inference over a factor graph that represents tampering models.
.

Keywords

Image Security, Image digest, image authentication, digital image processing

1. INTRODUCTION

Digital image processing is the technology of applying a number of computer algorithms to process digital images. The outcomes of this process can be either images or a set of representative characteristics or properties of the original images. The applications of digital image processing have been commonly found in robotics/intelligent systems, medical imaging, remote sensing, photography and forensics. The image processing directly deals with an image, which is composed of many image points. These image points, also namely pixels, are of spatial coordinates that indicate the position of the points in the image, and intensity (or gray level) values. A colorful image accompanies higher dimensional information than a gray image, as red, green and blue values are typically used in different combinations to reproduce the colors of the image in the real world.

The main purpose of digital image processing is to allow human beings to obtain an image of high quality or descriptive characteristics of the original image. In addition, unlike the human visual system, which is capable of adapting itself to various circumstances, imaging machines or sensors are reluctant to automatically capture "meaningful" targets. For example, these sensory systems cannot discriminate between a human subject and the background without the implementation of an intelligent algorithm.

The digital images are being widely used in numerous applications such as military, intelligence, surveillance, digital copyright applications, etc. Among the existing image formats, JPEG is the most widely used formats that stores the digital images using digital cameras and software tools. With the increase in use of multimedia type data over the internet. The Image authentication plays an important role in security and communication. Images are being transferred over the Internet and are readily available for access from any part of the world and without introducing an authentication mechanism, it is almost impossible to distinguish if an image is original or being manipulated.

Using cryptographic methods to authenticate image data will result in an unworkable system or unacceptable systems because data authentication is sensitive to single bit change in the original data while image authentication systems need to be mainly content sensitive. This is because images undergo a range of processing including lossy compression that result in changes in bits that are deemed acceptable. Such changes must be tolerable by the authentication system while it is essential for the system to remain sensitive to malicious manipulations. Many organizations are struggling with the issue of photo tampering. For example, digital images, videos, and audio are now routinely introduced as evidence in civil, criminal, and national security cases. In such cases, the integrity of digital evidence is central.

2. LITERATURE SURVEY

In year 2010, E Kee et. al. proposed a method [29] that describes how to exploit the formation and storage of an embedded image thumbnail for image authentication. The creation of a thumbnail is modeled with a series of filtering operations, contrast adjustment, and compression. We automatically estimate these model parameters and show that these parameters differ significantly between camera manufacturers and photo-editing software. We also describe how this signature can be combined with encoding information from the underlying full resolution image to further refine the signature's distinctiveness.

Past approaches for image authentication fall into three groups: forensics, watermarking, and robust hashing. In digital forensics, the user verifies the authenticity of an image solely by checking the received content [8] – [9]. Unfortunately, without any information from the original, one cannot completely confirm the integrity of the received content because content unrelated to the original may pass forensic checking. Another option for image authentication is watermarking. A semi-fragile watermark is embedded into the host signal waveform without perceptual distortion [10]–[11]. Users can confirm authenticity by extracting the watermark from the received content. The system design should ensure that the watermark survives lossy compression, but that it breaks as a result of malicious manipulations. Unfortunately, watermarking authentication is not backward compatible with previously encoded contents; i.e., unmarked content cannot be authenticated later. Embedded watermarks might also increase the bit rate required when compressing a media file.

Similarly Yao et. al. [11] developed an authentication techniques based on robust hashing, which is inspired by cryptographic hashing [13]. In this technique, the user checks the integrity of the received content using a small amount of data derived from the original content. Many hash-based image authentication systems achieve robustness against lossy compression by using compression-invariant features, such as [14]–[15]. These compressions-inspired features are designed for particular compression schemes but fail under other coding schemes or common image processing. Robustness is increased using more sophisticated features, such as block-based histograms [16], zero-mean low-pass Gaussian pseudo-random projection [17], [18], block standard deviations and means [17], [18], column and row projections [29], and transform coefficients [20], [21]. Any fixed projection has the weakness that an attacker who knows the null space of the projection can alter the image without affecting the authentication data. Using pseudo-random projections or tiling, such as in [22], keeps the null space a secret. Similar considerations apply to features calculated in a nonlinear manner. Features robust against rotation, cropping, resizing, or translation has been proposed based on the Radon transform [23]–[24], the Fourier transform [25], and pixel statistics along radii [25]–[26]. Other methods include features important to the human visual system [28].

Quantization and compression of authentication data have not been studied in depth. Most approaches use coarse quantization. For example, Fridrich et al. Use 1-bit quantization for random projection coefficients and the relation-based approaches can be considered as 1-bit quantizations of coefficient differences. The first to consider error-correcting coding in reducing the image authentication data size were Venkatesan et al. [21]. The idea is to project the binary feature vectors of both images into syndrome bits of an error-correcting code and directly compare the syndrome bits to decide the authenticity.

The approach of Sun et al. uses systematic Hamming codes to obtain the parity check bits of the binary feature vectors as the authentication data [30].

Therefore, after analyzing all the above research work, it is found that still this research area has a wide space of simple and effective techniques for image authentication. Hence, in this research work we proposed a mechanism for image authentication based on the encoding-decoding scheme of low density parity check methods along with the proper use of cryptology. The proposed methodology ensures that the image received at receiver side is original and un-tampered.

3. PROBLEM DEFINITION

The Objective of this proposed work is to implement a robust technique that works for the authentication of images that can recognize as small as possible changes in the altered image in comparison with the original image. Using the manipulation tools that are available on the internet it is easy to tamper the digital images without any trace. Therefore, verification of originality of images has become a challenging task. The early research in image forensics introduced digital watermarking and robust hashing in the original image for authentication.

4. PROPOSED WORK

In [31], we already proposed a technique for the image authentication using LDPC codes, Therefore, In the proposed authentication system shown in Figure 4, a pseudorandom projection (based on a randomly drawn seed KS) is applied to the original image x and the projection coefficients X are quantized to yield Xq. The authentication data are comprised of two parts, both derived from Xq. The Slepian-Wolf bit stream S (Xq) is the output of a Slepian-Wolf encoder based on low-density parity-check (LDPC) codes and the much smaller digital signature D (Xq, KS) consists of the seed KS and a cryptographic hash value of Xq signed with a private key.

The authentication data are generated by a server upon request. Each response uses a different random seed KS, which is provided to the decoder as part of the authentication data. This prevents an attack which simply confines the tampering to the null space of the projection. Based on the random seed, for each 16x16 non overlapping block Bi,wegeneratea16x16 pseudorandom matrix Pi by drawing its elements independently from a Gaussian distribution N(1, σ 2p) and normalizing so that ||Pi||2 =1. We choose σ p =0.2 empirically. In this way, we maintain the nice properties of the mean projection as suggested in the previous section while gaining sensitivity to high-frequency attacks. The inner product +Bi,Pi, is quantized into an element of Xq. The rate of the Slepian-Wolf bit stream S(Xq) determines how statistically similar the target image must be to the original to be declared authentic. If the conditional entropy H(Xq|Y) exceeds the bit rate R in bits per pixels, Xq can no longer be decoded correctly. Therefore, the rate of S(Xq) should be chosen to distinguish between the different joint statistics induced in the images by the legitimate and tampered channel states. At the encoder, we select a Slepian-Wolf bit rate just sufficient to authenticate both legitimate 30 dB JPEG2000 and JPEG reconstructed versions of the original image.

At the receiver, the user seeks to authenticate the image y with authentication data S(Xq)and D(Xq,Ks). It first projects y to Y in the same way as during authentication data generation. A Slepian-Wolf decoder reconstructs Xq & from the Slepian-Wolf bit stream S(Xq) using Y as side information. Decoding is via the LDPC message- passing algorithm initialized according to the statistics of the legitimate channel state at the worst permissible quality for the given original image. Finally, the image digest of Xq' is computed and compared to the image digest, decrypted from the digital signature D(Xq,Ks) using a public key. If these two image digests do not match, the receiver recognizes that image y is tampered, otherwise the receiver makes a decision.

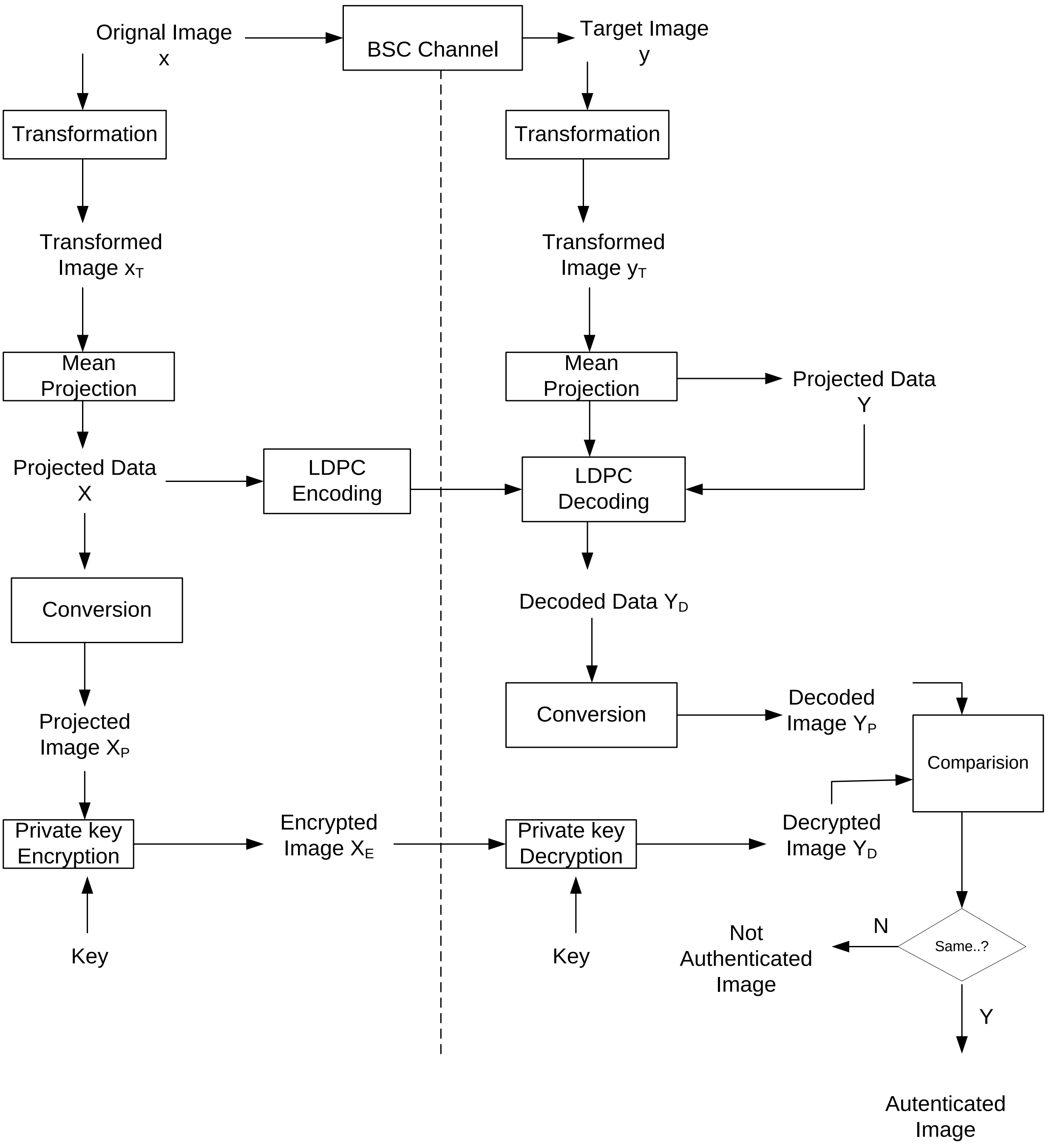

Fig 1: Proposed Image Authentication System

5. RESULTS

The experimental results reported in this section are performed on a system with Intel Core i5 processor and 6 GB RAM. The OS is Windows 7 Ultimate. Simulation software used is MATLAB 10.0 - R2010b (64 bit). The simulation results of the tampering localization decoder. In practice, the localization decoder would only run if the authentication decoder deems an image to be tampered, therefore, we perform multiple tests for the tampering localization system only with maliciously tampered images.

For the result analysis, we used the test images of 336 x 336 resolutions in 8-bit grey scale resolution. The authentic test images are BMP, JPEG or JPEG2000 compressed and reconstructed at several qualities. The malicious attack consists of the overlay of text banners at a random location in the image or removing a randomly selected Maximally Stable Extremes Region (MSER) by interpolating the region. For the text banners, the text color is white or black, whichever is more visible, to avoid generating trivial attacks, such as white text on a white area.

Using this data set, we demonstrate the performance of the authentication system for compressed images, the authentication system with a regular LDPC decoder for adjusting images, and the tampering localization system.

Following are the tables & corresponding figures for comparing the values of minimum decodable rate for both the cases i.e., Legitimate State & Tampered State.

Table 1: PSNR for fixed length coding, minimum decodable rates for tampered state DSC and minimum decodable rates for legitimate state DSC

S. No.	PSNR (dB)	Fixed Length Coding	Min Decodable Rate for tampered state with DSC	Min Decodable Rate for legitimate state with DSC
1	30	0.016	0.014	0.008
2	32	0.015	0.014	0.008
3	34	0.015	0.013	0.006
4	36	0.014	0.013	0.006
5	38	0.014	0.012	0.005
6	40	0.014	0.011	0.005

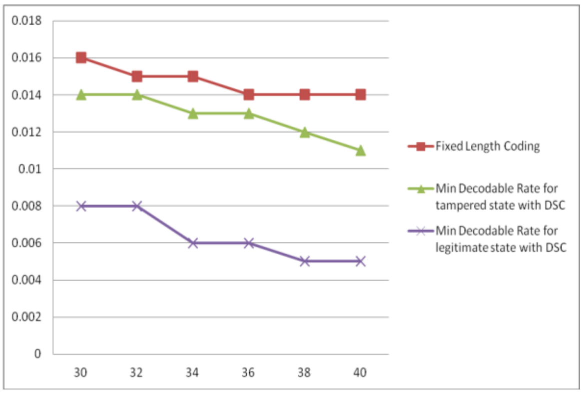

Fig 2: Minimum rates averaged for the tampered states for correctly decoding Slepian-Wolf bit stream for the images from database with the quantized projection X.

Table 2: Comparison of Authenticated Data size using DSC, Conventional FLC and compressed mean projection

S. No.	Authenticate Data Size (Bytes)	Distributed Source Coding	Conventional Fixed Length Coding	Compressed Mean Projection
1	000	0.08	0.12	0.13
2	200	0.08	0.12	0.13
3	400	0.06	0.10	0.12
4	600	0.05	0.09	0.09
5	800	0.04	0.09	0.09
6	1000	0.04	0.08	0.08

In figure below Graph shows that the ROC equal error rate versus the authentication data size and demonstrates that distributed source coding reduces the data size by more than compared to conventional fixed length coding at an equal error rate. Distributed source coding also outperforms a baseline authentication based on compressed mean projection. The encoder of this system uses the coefficients of a 16×16-block mean projection. Whereas figure 6 shows that the receiver operating characteristic (ROC) curves for tampering detection with different numbers of bits in quantization using distributed source coding, conventional fixed length coding and compressed mean projection. It shows that higher quantization precision offers better detection performance.

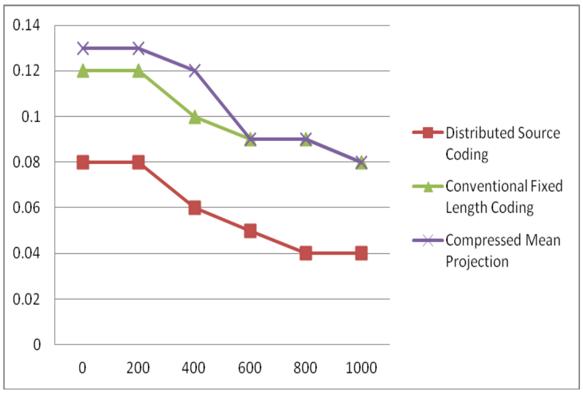

Fig 3: Graph shows that the ROC equal error rate versus the authentication data size and demonstrates that distributed source coding reduces the data size by more than compared to conventional fixed length coding at an equal error rate. Distributed source code.

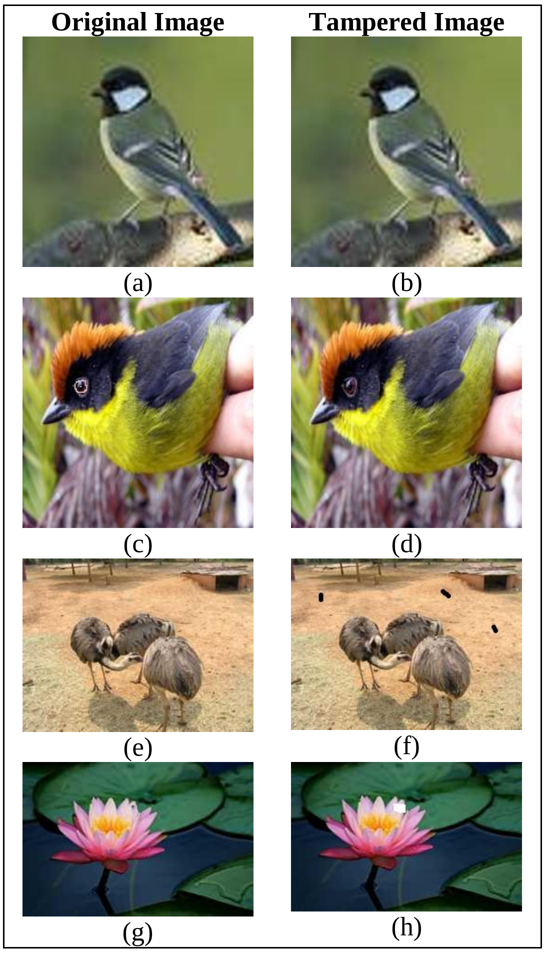

Fig 4: Images taken during experiments

6. CONCLUSION

In This paper we analyzes the previous work done in the same domain and proposes a novel image authentication scheme that distinguishes legitimate encoding variations of an image from tampered versions based on distributed source coding and statistical methods. A two-state lossy channel model represents the statistical dependency between the original and the target images. Tampering degradations are captured by using a statistical image model, and legitimate compression noise is assumed to be additive white Gaussian noise.

7. REFERENCES

[1]. J. Fridrich, D. Soukal, and J. Luk´aˇs, “Detection of copy move forgery in digital images,” in Proceedings of Digital Forensic Research Workshop, August 2003.

[2]. A. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Tech. Rep. TR2004-515, Department of Computer Science, Dartmouth College, 2004.

[3]. Z. Lin, R. Wang, X. Tang, and H.-V. Shum, “Detecting doctored images using camera response normality and consistency,” in Computer Vision and Pattern Recognition, (San Diego, CA), 2005.

[4]. M. Johnson and H. Farid, “Exposing digital forgeries in complex lighting environments,” IEEE Transactions on Information Forensics and Security 3(2), pp. 450–461, 2007.

[5]. J. Luk´aˇs, J. Fridrich, and M. Goljan, “Digital camera identification from sensor noise,” IEEE Transactions on Information Security and Forensics 1(2), pp. 205–214, 2006.

[6]. Gallager, R. G., “Low Density Parity Check Codes, Monograph”, M.I.T. Press, 1963

[7]. H. Farid, “Image forgery detection,” IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, Mar. 2009.

[8]. A. Popescu andH. Farid, “Exposing digital forgeries in color filter array interpolated images,” I EEE Trans. Signal Process., vol. 53, no. 10, pp. 3948–3959, Oct. 2005.

[9]. I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure sprectrum watermarking for images, audio and video,” in Proc. I Conf. Image Process., Lausanne, Switzerland, Sep. 1996.

[10]. R. B. Wolfgang and E. J. Delp, “A watermark for digital images,” in Proc. IEEE Int. Conf. Image Process., Lausanne, Switzerland, Sep.1996

[11]. Yao-Chung Lin, David Varodayan, “Image Authentication Using Distributed Source Coding” In IEEE Transactions On Image Processing, Vol. 21, No. 1, January 2012, Pp.273-283

[12]. W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Jan. 1976.

[13]. C.-Y. Lin and S.-F. Chang, “Generating robust digital signature for image/video authentication,” in ACM Multimedia: Multimedia and Security Workshop, Bristol, U.K., Sep. 1998, pp. 49–54.

[14]. M. Schlauweg, D. Pröfrock, and E. Müller, “JPEG2000-based secure image authentication,” in Workshop on Multimedia and Security, Geneva, Switzerland, 2006, pp. 62–67.

[15]. M. Schneider and S.-F. Chang, “A robust content based digital signature for image authentication,” in Proc. IEEE Int. Conf. Image Process., Sep. 1996, vol. 3, pp. 227–230.

[16]. J. Fridrich, “Robust bit extraction from images,” in Int. Conf. Multimedia Computing and Syst., Jul. 1999, vol. 2, pp. 536–540.

[17]. D.-C. Lou and J.-L. Liu, “Fault resilient and compression tolerant digital signature for image authentication,” IEEE Trans. Consumer Electronics, vol. 46, no. 1, pp. 31–39, Feb. 2000.

[18]. L. Xie, G. R. Arce, and R. F. Graveman, “Approximate image message authentication codes,” IEEE Trans. Multimedia, vol. 3, no. 2, pp.242–252, Jun. 2001.

[19]. R.-X. Zhan, K. Y. Chau, Z.-M. Lu, B.-B. Liu, and W. H. Ip, “Robust image hashing for image authentication based on DCT-DWT composite domain,” in Proc. IEEE Int. Conf. Intelligent Syst. Design and Application., Nov. 2008, vol. 2, pp. 119–122.

[20]. H. Zhang, H. Zhang, Q. Li, and X. Niu, “Predigest Watson’s visual model as perceptual hashing method,” in Int. Conf. Convergence and Hybrid Inf. Technol., Nov. 2008, vol. 2, pp. 617–620.

[21]. R.Venkatesan, S.-M.Koon,M.H. Jakubowski, and P.Moulin, “Robust image hashing,” in Proc. IEEE Int. Conf. Image Process., 2000, vol. 3, pp. 664–666.

[22]. F. Lefebvre, J. Czyz, and B. Macq, “A robust soft hash algorithm for digital image signature,” in Int. Conf.Multimedia and Expo, Baltimore, MD, 2003.

[23]. H.-L. Zhang, C.-Q. Xiong, and G.-Z. Geng, “Content based image hashing robust to geometric transformations,” in Proc. Int. Symp. Electronic Commerce and Security, May 2009, vol. 2, pp. 105–108.

[24]. A. Swaminathan, Y. Mao, and M. Wu, “Robust and secure image hashing,” IEEE Trans. Inf. Forensics and Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[25]. C. De Roover, C. DeVleeschouwer, F. Lefebvre, and B.Macq, “Robust video hashing based on radial projections of key frames,” IEEE Trans. Signal Process., vol. 53, no. 10, pp. 4020–4037, Oct. 2005.

[26]. Z. Tang, S.Wang, X. Zhang, andW.Wei, “Perceptual similarity metric resilient to rotation for application in robust image hashing,” in Proc. Int. Conf. Multimedia and Ubiquitous Eng., Jun. 2009, pp. 183–188.

[27]. V. Monga and B. L. Evans, “Perceptual image hashing via feature points: Performance evaluation and tradeoffs,” IEEE Trans. Image Process., vol. 15, no. 11, pp. 3452–3465, Nov. 2006.

[28]. M. Schlauweg and E. Müller, “Gaussian scale-space features for semi-fragile image authentication,” in Proc. Picture Coding Symp., May 2009, pp. 1–4.

[29]. E Kee, H Farid, “Digital Image authentication from thumbnails” In SPIE symposium on electronic imaging, San Jose, CA, 2010

[30]. M.Tagliaasacchi, G. Valensize, and S. Tubaro, “Hash Based identification of spase image tampering”, IEEE trans, image process, vol. 18 no. 11, pp. 2491-2504, Nov. 2009.

[31]. Imran A khan, “An overview to the proposed technique for image authentication using LDPC codes”, IJCST Vol.4, Jan 2013.