ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 347 - 353 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp65.pdf

Watermarking marking technique used for tampering Detection in compressed digital video

S.Aswini[1], M.Tech (DSCE), Dept. of E.C.E, S.V.Engineering for women,Tirupati,
aswini.sivanandam04@gmail.com
A.Hazarathaiah[2], Professor, Head of the dept. of E.C.E, S.V.Engineering for women, Tirupati,
hazarath.a@svcolleges.edu.in

***Abstract*— Dynamically introduces a system to identify feature altering and recognize it from normal feature handling operations, for example, re compression, commotion, and splendor build, utilizing a commonsense watermarking plan for ongoing validation of advanced feature. In our strategy, the watermark signs speak to the macro block's and outline's records, and are inserted into the nonzero quantized discrete cosine change estimation of squares, generally the last nonzero qualities, empowering our system to recognize spatial, worldly, and spatio temporal altering. Our strategy can be effortlessly arranged to alter straightforwardness, power, and limit of the framework as indicated by the particular application nearby. What's more, our strategy exploits substance based cryptography and expands the security of the framework. While our system can be connected to any current feature codec, including the as of late discharged high-effectiveness feature coding standard, we have actualized and assessed it utilizing the H.264/AVC codec, and we have demonstrated that contrasted and the current comparable strategies, which likewise implant additional bits inside feature outlines, our strategy causes fundamentally littler feature twisting, prompting a PSNR corruption of around 38.7330dB and basic comparability file abatement of 0.0090 with just 0.05% expansion in bit rate, and with the bit rate of 0.71 to 0.88 after H.264/AVC recompression.**

I.INTRODUCTION

The quick development of the Internet, sudden generation of ease and solid stockpiling gadgets, computerized media creation, and altering advances have prompted far reaching frauds and unapproved sharing of advanced media. Among these media, feature is turning out to be progressively critical in an extensive variety of utilizations, for example, feature observation, feature telecast, DVDs, feature conferencing, and feature on-interest applications, where realness and uprightness of the feature information is essential. In reconnaissance applications, huge ventures have been made in framework, for example, camcorders and systems introduced in broad daylight offices on a wide scale. Nonetheless, current feature altering programming can be utilized to mess with such feature, making them untrustworthy and crushing the motivation behind such applications at the primary spot. Without confirmation, a feature viewer (or a shopper) can't check that the feature being seen is truly the first one that was transmitted by a maker. There may be a few meddlers who alter the feature content purposefully to damage the hobbies of either or both the maker and the buyer. There is in this manner a need to recognize such tampering, as well as to recognize them from normal feature handling operations, for example, pressure. As a symptom, feature confirmation can likewise be utilized for notice checking, where an organization can naturally recognize, progressively, regardless of whether a particular TV or Internet channel has cut a couple edges of the organization's promotion to acquire time and cash. Considering these diverse applications, validation frameworks are getting to be prevalent to guarantee the honesty of feature substance.

No doubt understood answers for the above issues are watermarking, which stows away critical data in the media. An all around outlined watermarking framework must give three fundamental elements: 1) straightforwardness; 2) strength; and 3) limit. Straightforwardness implies that the checked sign ought to be perceptually proportional to the first flag; strength alludes to a dependable extraction of the watermark regardless of the fact that the stamped sign is debased, and limit is a measure of the amount of data can be implanted into the media. While the first inspiration driving watermarking was copyright assurance, watermarking can likewise be utilized for checking the genuineness and trustworthiness of the feature by implanting the watermark data behind a spread. The implanted watermark can then be distinguished or removed from the spread feature utilized for confirmation.

Rather than vigorous watermarking, which is intended for copyright security, delicate watermarking has been intended for alter recognition. An assailant's objective in altering is to change the watermarked media while keeping the watermark itself untouched, to trap the collector into accepting

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 347 - 353 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp65.pdf

that the altered media is credible and has respectability. While delicate watermarking can ensure against such an assault, it is exceptionally touchy to alterations, making it hard to recognize malignant altering from some normal feature handling operations, for example, recompression. To adventure the benefits of both the vigorous and the delicate plans, semi fragile watermarking has been proposed to endure regular handling, for example, recompression, and in the meantime identify noxious altering.

We present a watermarking plan that can be utilized to recognize malignant altering. Our plan can be utilized as a part of any current feature codec, and can survive pressure by cutting edge codec's, for example, H.264/AVC, though numerous current altering location plans are delicate against H.264/AVC pressure.

In our proposed plan, macroblock's' (MBs') and outlines' files are inserted into the last nonzero (LNZ) quantized discrete cosine change (QDCT) estimation of the squares. Utilizing high recurrence levels drives us to guarantee straightforwardness to the human visual framework. Contrasted and the current H.264/AVC watermarking plans, our answer has five advantages: 1) it addresses both spatial and transient spaces, which prompts identifying different pernicious changes in spatial and time areas; 2) it is speedier and with lower multifaceted nature contrasted with existing calculations, making it commonsense and suitable for continuous applications; 3) its execution is basic and obliges minor changes in the codec; 4) it gives high straightforwardness and high limit; and 5) the forced bit rate increment for the packed H.264/AVC bit stream is for all intents and purposes almost zero (around 0.05%), dissimilar to existing plans that build the bit rate fundamentally, generally in the 3%–15% territory.

In this paper, we have extended our outline and now insert the watermark flags in the LNZ values, as well as in other nonzero quantized discrete cosine change (DCT) estimation of pieces, incorporating those in the center or even low frequencies. This expands the security of our plan and makes it more troublesome for an interloper to imperceptibly mess around with the feature, albeit actually it additionally builds bending. We have additionally enhanced the bit rate overhead from 3.6% to just 0.05% in this paper. At last, in this paper, we are displaying exhaustive assessments of our calculation and treating essentially adding to or growing the assessment.

II. Proposed Watermarking Scheme

While the proposed plan can be utilized for all feature watermarking applications, for example, copyright security, in this paper, we concentrate on validation and altering identification. Every application, including confirmation, has its own necessities. With the prerequisites of a verification application, here we outline a semi fragile watermarking technique. The rundown of our configuration is as per the following.

The majority of the customary watermarking plans are not powerful against pressure, particularly HEVC or H.264/AVC pressure, and after pressure, the mystery implanted data is not recognizable. Conversely, our proposed plan exploits the pressure standard to insert and concentrate mystery bits. Subsequent to performing DCT and the quantization stages, almost 4×4 squares of every 16×16 MB are chosen for inserting. With the quantity of mystery bits which will be inserted into a MB, the quantity of chose squares is picked. In each MB, the obstructs that have bigger LNZ level position are chosen, i.e., hinders that have the most elevated high recurrence test. Picking high-recurrence QDCT qualities forces lower adjustment contortion. In each chose obstruct, a solitary mystery bit is implanted. In the event that the comparing mystery bit is zero, the total of all levels ought to be even. On the off chance that it is odd, the LNZ level is increased or decremented by one. On the off chance that the mystery bit is one, the aggregate ought to be odd. Notwithstanding, if the whole is even, the LNZ level ought to be increased or decremented by one. For expanded vigor, we likewise utilize some other nonzero levels, however at a tradeoff with expanded twisting.

The trial results demonstrate that the proposed plan is straightforward, high limit, and powerful against regular sign handling operations. Selecting pieces taking into account the recurrence tests prompts a versatile feature watermarking framework with its ability, straightforwardness, and heartiness balanced effectively.

In our proposed technique, the record of each MB is implanted within it; likewise, the list of every casing is inserted into the present edge. Along these lines, this plan gives a decent answer for both spatial and worldly altering. H.264/AVC recompression, commotion, sifting, and other spatial changes cause a few blunders in alter discovery. Nonetheless, in our plan, investigating the extraction blunder will recognize noxious assaults from basic preparing, for example, pressure. Furthermore, extricated outlines' files help us to perceive any edge control, for example, including additional edges, reordering, dropping, or substitution of feature casings. Because of the above rundown, let us now examine the subtle elements of our configuration, beginning with a few definitions furthermore, and clarifications of related idea

A. Tampering

Feature altering plans can be grouped into spatial altering, transient altering, or mix of them. Spatial altering, likewise called intra casing altering, alludes to changing the

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 347 - 353 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp65.pdf

picture edge, for example, trimming and substitution, substance including an evacuation. Fleeting altering, likewise named bury casing altering, is the progressions set aside a few minutes area, for example, including additional edges, reordering the grouping of casings, dropping, and supplanting edges. Because of transient repetition in feature information, it is conceivable to perform fleeting altering without forcing visual bending and semantic modification. Therefore, having a confirmation framework for fleeting altering identification is certain.

B. Transparency, Capacity, and Robustness

The watermarking procedure ought not bring any noticeable antiquities into the first substance. Preferably, there must be no discernible distinction between the watermarked and the first computerized substance, i.e., the watermark information ought to be straightforward to the client. Aside from straightforwardness, limit and vigor are two other central properties of feature watermarking. Limit is characterized as the quantity of bits installed in one second of the feature. For power, the watermark ought to be extractable after different deliberate or unexpected assaults. These assaults may incorporate added substance commotion, resizing, low-pass sifting, and whatever other assault, which may evacuate the watermark or confound the watermark extraction framework. The tradeoff between limit, straightforwardness, and vigor is the primary test for feature watermarking applications, i.e., in a perfect case, we would request an exceptionally straightforward, vigorous, and high-limit plan. Nonetheless, by and by, acquiring every one of these properties in the meantime is amazingly troublesome or even outlandish. Consequently, contingent upon the prerequisites of the specific application within reach, a tradeoff between these properties must be accomplished.

Considering this tradeoff, the accompanying sorts of watermarking plans lead to diverse limit, straightforwardness, and heartiness.

1) Fragile: Very high limit and straightforwardness can be accomplished.

2) Semi fragile: Robustness against pressure and normal sign handling operations is gotten. For this situation, it is acknowledged that more contortion is brought on contrasted and delicate watermarking. The fundamental utilization of this classification is verification, which is the primary focus of this paper.

3) Robust: Robustness against numerous assaults with an extensive variety of changes is accomplished. This is more confused than the past two sorts, since we require strength against the greater part of the assaults. Along these lines, as indicated by the exchange off between limit, straightforwardness, and vigor, a penance in limit and straightforwardness is made. The principle utilization of this class is copyright security.

Our proposed plan exploits the codec to install the mystery data with the goal that watermarking can be identified at the decoder side, i.e., inserting the watermark is a piece of the feature encoding procedure. Utilizing the encoder takes care of the issue of strength against pressure furthermore prompts low multifaceted nature since the proposed system utilizes DCT pieces, which are as of now registered by all present day feature encoders, including HEVC and H.264/AVC. In our proposed system, QDCT coefficients (otherwise called levels) of a few squares are controlled to install the watermark signals.

C. Embedding

Embedding Implanting in the low recurrence levels of 4 × 4 pieces, which convey perceptually essential data, brings about evident quality contortion in the watermarked feature. Thusly, in our proposed plan, we basically utilize the most recent nonzero QDCT coefficients of 4×4 pieces, named LNZ levels, which are in the high or mid frequency groups to install the watermark. For expanded power, we additionally utilize some other nonzero levels, however at a tradeoff with expanded bending. In every 16 × 16 MB, we implant ($k < 16$) bits. Truth be told, k 4 ×4 hinders among the 16 pieces of each MB are chosen for implanting, while a solitary bit is installed in each chosen square. On the off chance that all levels in a square are zero and there is no LNZ, as can happen in high QP values, we can't insert inside that piece. Subsequently, before picking k, the quantity of hinders that have LNZ ought to be considered. The implanting procedure is performed after the quantization stage by taking after the progressions beneath, which prompt inserting k bits in the current MB.

.

1) For every 4 × 4 piece inside of the current MB, discover the position of the LNZ level.
2) Select k hinders that have LNZ levels in higher positions, call them block i (i = 1 to k). As it were, we select hinders that have high recurrence levels. Case in point, a piece with its LNZ level situated at position 12 has need over another square with its LNZ level at position 3.
3) To enhance the security, the verification code As, is encoded by a key called C, to frame the watermark signal W

$$W=E(C, As)$$

Where E is the encryption operation, and As is the twofold MB number with a length of k bits. In the trial results, since we have utilized QCIF cuts (176 × 144), there are 99 MBs in every casing that should be stamped.
To create 99 numbers, seven bits are obliged ($k \geq 7$).
4) In each MB, do step 5 for each chose block i . In the event that a piece is not chosen for inserting, it ought to be left as seems to be.

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 347 - 353 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp65.pdf

5)) For each chose block i , process the entirety, Si, of all levels inside of the square and change its LNZ level (Li) taking into account Si and wi , as takes after:

$$L_i = \begin{cases} L_i + 1 & \text{if } S_i \text{ is odd}, W_i \text{ is zero and } L_i \neq -1 \\ L_i - 1 & \text{if } S_i \text{ is odd}, W_i \text{ is zero and } L_i = -1 \\ L_i & \text{if } S_i \text{ is odd}, W_i \text{ is one} \\ L_i & \text{if } S_i \text{ is even}, W_i \text{ is zero} \\ L_i + 1 & \text{if } S_i \text{ is even}, W_i \text{ is one and } L_i \neq -1 \\ L_i - 1 & \text{if } S_i \text{ is odd}, W_i \text{ is zero and } L_i = -1 \end{cases}$$

Where wi is the watermark bit of block i and L_ i is the stamped LNZ level of chose block i.

At the extraction stage in the decoder, the position of the LNZ level is expected to distinguish the chose pieces. In this way, the nonzero levels ought not be changed to zero. Hence, if the level quality is equivalent to −1, it ought to be decremented rather on being augmented in the event that it needs to change.

To make our plan hearty against agreement assaults, as opposed to utilizing a novel key as a part of step 3, the key is produced in view of MBs elements. These components should be sufficiently vigorous to evade the likelihood of varieties in the wake of reencoding. To counteract computational many-sided quality, we utilized the codec data for creating a key for each MB. In 4 × 4 intraprediction, nine modes are characterized into three gatherings:
1) Vertical and inclining modes (0, 3, 4, 5, 7); 2) even modes (1, 6, 8); and 3) dc mode
(2)As comparative modes may be changed to one another after re-encoding, arranging them makes general society enter more vigorous if there should arise an occurrence of shifts. For three modes, two bits are required and doled out for every mode. In this manner, a 32-bit substance based key is created for a MB, which incorporates 16 4 × 4 squares. Also, for 16 × 16 intraprediction, there are four modes for which, taking into account the expectation mode, a 32-bit substance based key is made. For instance, in 4 × 4 intraprediction, for the to begin with, second, and third gatherings, we can allocate 00, 01, and 10, individually. Also, a 32-bit key that begins with 11 can be utilized for 16 × 16 intraprediction mode.

A few procedures may change the intraprediction modes in pieces, which thusly prompt diverse level qualities, and in this way make the installed watermark imperceptible. Subsequent to reencoding, the luma forecast modes may be changed, which influences the synchronization in the watermark extraction process. To assess this impact, we considered the rate of forecast mode changes subsequent to reencoding. As it is demonstrated in Table I, when the quantity of nonzero levels builds, the likelihood of changes in intramodes diminishes. As it were, more textured squares can withstand better against the reencoding procedure and, accordingly, against different controls. These coefficients for the most part compare to nonflat territories, which are more helpless against assaults since aggressors intend to change the surface ranges, not the foundation.

As we characterize intraprediction in gatherings and dole out two bits to every gathering, the likelihood of gathering change is even not as much as changes in modes. In this way, the key can be separated in the majority of the cases.

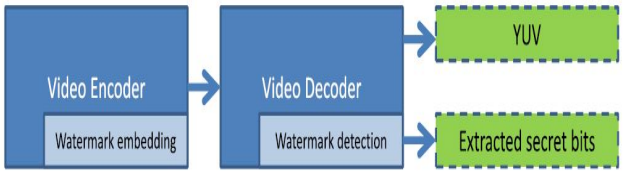

Fig. 1. Embedding and detecting flowchart.

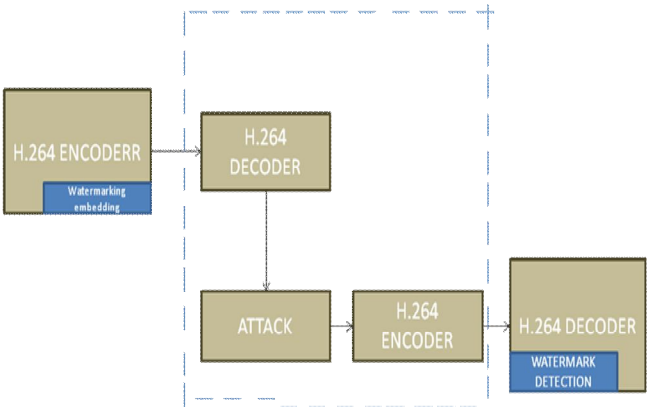

Fig.2. Flowchart for embedding, attack, and detection.

The inserting procedure does not modify the quantity of levels, which serves to keep the bit rate the same as the first without watermark implanting. Fig. 1 demonstrates the implanting and distinguishing methodology. In the wake of disentangling the stream, which incorporates watermark recognition, the YUV information and the removed mystery bits are gotten.

We can undoubtedly modify the properties of our watermarking framework. By expanding k, the limit is expanded yet straightforwardness and strength are diminished. Expanding k implies utilizing more pieces as a part of each MB for implanting, which thus brings the mistake rate up in the event of assaults or basic handling operations. Hence, expanding k diminishes power of the framework.

To uproot excess, pressure calculations control high-recurrence components more, since the human perceptual framework is delicate to changes in center and low frequencies. To enhance vigor, as opposed to installing the watermark in just the LNZ levels (the most astounding recurrence), different levels in the center or even low frequencies can be utilized for inserting, despite the fact that the contortion for this situation would increment. At the point when the LNZ levels as well as other nonzero levels are

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 347 - 353 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp65.pdf

utilized for installing, the limit of the framework is expanded and it turns out to be more troublesome for an aggressor to track the progressions.

In H.264/AVC pressure, changing the quantization parameter (QP) brings about shifting the quantity of nonzero levels in MBs. It is apparent that when QP is low, there are more nonzero levels contrasted and high QP. In this way, if QP is low, we can insert 16 bits in each MB and if QP is high, we can install under 16 bits in each MB. At the end of the day, if QP is high and pressure rate is high (i.e., the feature is exceptionally packed), we have to pick a suitable k (under 16). Hence, when QP is low, watermark installing will bring about not so much mutilation but rather more limit, and when QP is high, they gave limit is lower.

D. Detecting

The installed watermark bits are removed in the feature disentangling procedure where the quantized DCT levels for each MB are entropy decoded. For each MB, the accompanying steps bring about extricating k inserted bits from each MB.

1) Sort the position estimations of the LNZ levels for 16 pieces of the current MB. At that point, select k hinders that have higher nonzero position values and are utilized for implanting.

2) In each of the above chose obstructs, a bit is inserted, which can be separated as takes after:

$$W_i' = \begin{cases} 0 \text{ if } S_i' \text{ is even} \\ 1 \text{ if } S_i' \text{ is odd} \end{cases}$$

Where w_i is the removed bit of the i th chose piece of the current MB in the decoder and Si is the aggregate of all levels in the i th chose square of the current MB in the decoder.

To accomplish the crude watermark stream for each MB, we have to utilize the encryption key of the ebb and flow MB. This key was created in view of intraprediction modes in the encoder, which can be recovered in the decoder too.

By and large, effectiveness, many-sided quality, vitality use, and effortlessness are more critical in the decoder usage since it is at the customer side with restricted assets contrasted and the server side, which has more assets. Likewise, some deferral in the encoder is adequate since it is done once for a feature. Therefore, low many-sided quality and straightforwardness in execution are discriminating focuses in outlining the decoder. One point of preference of our proposed method is its straightforwardness of execution at the decoder side, permitting it to keep running for different ongoing

With this security scheme, an attacker has following difficult challenges to avoid tamper detection.

1) The attacker needs to have both the original and marked video to find the modified QDCT values. This is highly unlikely that an attacker can access the original video to discover the changes.

2) In the very rare case that an attacker has access to the original video clip and finds the modified QDCT, the attacker must keep the LNZ level and change the other

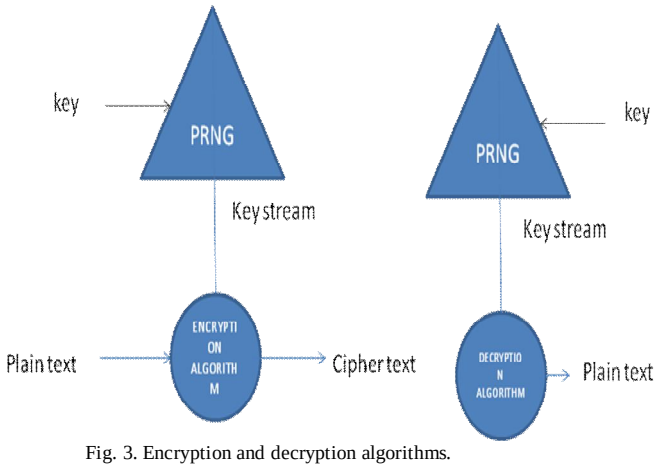

Fig. 3. Encryption and decryption algorithms.

Levels to prevent tamper detection. However, this is very difficult, if not practically impossible, because:

a) The embedding and extracting processes work based on the sum of all levels in each selected block;

b) The encryption key is generated based on the levels and content of the blocks. Thus, any change in the levels will be detected at our tamper detection phase.

Therefore, it is practically impossible for an attacker to bypass the tampering detection stage

III. EXPERIMENTAL RESULTS

Although our scheme can be used in any DCT-based video encoder, as a proof-of-concept, we have specifically implemented and integrated our scheme with the H.264/AVC, although the presented results will be similar in other modern video codec's as well, and our conclusions are without loss of generality.

Taking the following video sequences in QCIF format (176 × 144 pixels) are used for our simulations. Since we embed the watermark in 16×16 MBs, our algorithm is independent of the resolution of the video, so there is no need to test higher resolution formats

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 347 - 353 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp65.pdf

(a) **(b)**

Fig 4.(a). Unmarked H.264/AVC compressed/decompressed frames, (b) Marked H.264/AVC compressed/decompressed frames

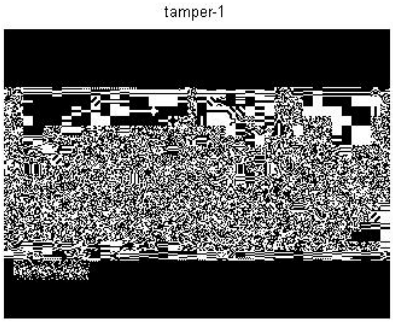

Fig.5. The difference between the unmarked and marked decoded frames

Fig.6.Extracted hidden data from the Input video.

Fig.7. Final video after the tamper detection

While PSNR is a very popular and widely used evaluation method, it is known that its correlation to subjective quality measures is not always good, because it reflects only the luminance component and neglects the chrominance component, which is important to human perception. Therefore, in addition to PSNR, we have also used the structural similarity index (SSIM).
Used 42.684 percent of the source image. 1 extracted secret data successfully.

MSError =0.0079, sd = 2.9620, PSNR = 38.7330dB

IV.CONCLUSION

A commonsense arrangement of computerized feature watermarking is proposed for confirming and altering location of packed features. To outline a proficient and low-intricacy technique, the inserting and extricating of watermarks are incorporated with the coding and interpreting schedules of the feature codec. To guarantee straightforwardness to the human visual framework, the MBs' and outlines' lists are inserted into the LNZ quantized DCT estimation of the squares. The recommended confirmation system gives discovery of spatial, transient, what's more, spatiotemporal altering. The exploratory results show that the mutilation created by our framework is low overall, PSNR is 38.7330 dB, SSIM is −0.0090, expanding bit rate is only 0.05%, and BCR after H.264/AVC recompression is 0.71–0.88. Including substance based cryptography to the watermarking framework builds the security of the framework and marginally diminishes BCR (1% to 5%) after H.264/AVC recompression. Furthermore, to distinguish malicious attacks from common video processing operations, such as H.264/AVC recompression, noise, and brightness increasing, analysis of the error is used to detect tampering.

V.REFERENCES

[1] S. Chen and H. Leung, “Chaotic watermarking for video authentication in surveillance applications,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 5, pp. 704–709, May 2008.

[2] P.-C. Su, C.-S. Wu, I.-F. Chen, C.-Y. Wu, and Y.-C. Wu, “A practical design of digital video watermarking in H.264/AVC for content authentication,” *Signal Process, Image Commun.*, vol. 26, nos. 8–9, pp. 413–426, Oct. 2011.

[3] D. Xu, R. Wang, and J. Wang, “A novel watermarking scheme for H.264/AVC video authentication,” *Signal Process., Image Commun.*, vol. 26, no. 6, pp. 267–279, 2011.

[4] C. Fei, D. Kundur, and R. H. Kwong, “Analysis and design of secure watermark-based authentication systems,” *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 43–55, Mar. 2006.

[5] J. Sang and M. S. Alam, “Fragility and robustness of binary phaseonly filter based fragile/semi-fragile digital image watermarking,” *IEEE Trans. Instrum. Meas.*, vol. 57, no. 3, pp. 595–606, Mar. 2008.

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 347 - 353 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp65.pdf

[6] M. Fallahpour, M. Semsarzadeh, S. Shirmohammadi, and J. Zhao, "A realtime spatio-temporal watermarking scheme for H.264/AVC," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, Minneapolis, MN, USA, May 2013, pp. 872–875.
[7] K. S. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality-preserving data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 10, pp. 1499–1512, Oct. 2009.
[8] R. Iqbal, S. Shirmohammadi, A. E. Saddik, and J. Zhao, "Compresseddomain video processing for adaptation, encryption, and authentication," *IEEE Multimedia*, vol. 15, no. 2, pp. 38–50, Apr./Jun. 2008.
[9] J. Zhao, W. J. Tam, S. Wang, D. Zheng, and F. Speranza, "A digital watermarking and perceptual model based video quality measurement," in *Proc. IEEE Conf. Instrum. Meas. Technol.*, May 2005, pp. 1729–1734.
[10] M. Barni, F. Bartolini, and N. Checcacci, "Watermarking of MPEG-4 video objects," *IEEE Trans. Multimedia*, vol. 7, no. 1, pp. 23– 32, Feb. 2005.
[11] S. Biswas, S. R. Das, and E. M. Petriu, "An adaptive compressed MPEG-2 video watermarking scheme," *IEEE Trans. Instrum. Meas.*, vol. 54, no. 5, pp. 1853–1861, Oct. 2005.
[12] S. N. Biswas, S. Nahar, S. R. Das, E. M. Petriu, M. H. Assaf, and V. Groza, "MPEG-2 digital video watermarking technique," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, May 2012, pp. 225–229.
[13] X. L. Chen and H. M. Zhao, "A novel video content authentication algorithm combined semi-fragile watermarking with compressive sensing," in *Proc. 2nd Int. Conf. Intell. Syst. Des. Eng. Appl.*, Sanya, Hainan,
China, Jan. 2012, pp. 134–137.
[14] Y. Shi, M. Qi, Y. Yi, M. Zhang, and J. Kong, "Object based dual watermarking for video authentication," *Int. J. Light Electron Opt.*, vol. 124, no. 19, pp. 3827–3834, 2013.
[15] C. L. Phillipsa, J. A. Anderson, and S. C. Glotzer, "Pseudo-random number generation for Brownian Dynamics and Dissipative Particle Dynamics simulations on GPU devices," *J. Comput. Phys.*, vol. 230, no. 19, pp. 7191–7201, Aug. 2011.