# Privacy-Preserving Watermarking Using PZM, SURF, QR Codes, and Visual Cryptography Against RST Attacks

**Kailash Chandra Totla**

M L V Textile & Engineering College, Bhilwara, India Country
Email - kctotla@gmail.com

***Abstract:*** *The fast development of digital multimedia has augmented concerns concerning to protection of copyright, data genuineness and the privacy preservation. This study presents a healthy privacy-preserving watermarking outline that mixes Pseudo-Zernike Moments (PZM), Speeded-Up Robust Features (SURF), QR code encoding and a four-share Visual Cryptography Scheme (VCS) to struggle Rotation, Scaling, and Translation attacks. PZM and SURF deliver invariant characteristics extraction and concurrent recovery under geometric alterations, whereas QR codes and VCS improve data safety through multi-layer defenses. The anticipated framework advances watermark sturdiness, safe information distribution and authentication trustworthiness. These proposals an active resolution for multimedia security submissions, with copyright protection, safe image distribution and electronic content verification.*

***Keywords:*** *Privacy-Preserving, Watermarking, PZM, SURF, QR Codes, Visual Cryptography.*

## 1. BACKGROUND AND MOTIVATION

The exponential development of digital media approaches has altered the method by which information is formed, stored and communicated. Images, videos and additional multimedia data might nowadays be distributed promptly across the sphere via the internet and various platforms of social networking. Whereas this progression has enhanced accessibility and communication, it has also familiarized grave concerns concerning to copyright infringement, unauthorized repetition, interfering and piracy. Subsequently, defending digital content has develop a serious research encounter in multimedia safety.

Digital watermarking has appeared as one of the furthermost operative methods for copyright fortification and ownership confirmation. In watermarking schemes, undisclosed information is entrenched into multimedia data and far along extracted to confirm the authenticity. Though, traditional watermarking techniques are often susceptible to geometric distortions like rotation, scaling and translation (RST) attacks. These attacks change the spatial assembly of a picture / image and interrupt synchronization among the entrenched watermark and the extraction procedure, leading to imprecise watermark detection.

To overwhelmed these boundaries, researchers have discovered advanced characteristics of extraction and cryptographic methods. Pseudo-Zernike Moments (PZM) deliver robust invariance in contradiction of noise and rotation, whereas Speeded-Up Robust Features (SURF) empower reliable discovery of local image features under geometric transformations. Additionally, Visual Cryptography Schemes (VCS) and QR code-based encryption procedures improve privacy and secure sharing of information. The amalgamation of these knowledges produces an all-inclusive framework proficient of delivering vigorous watermark defenses and improved security in multimedia atmospheres.

## 2. ROBUST FEATURE REPRESENTATION THROUGH PSEUDO-ZERNIKE MOMENTS AND SURF

The feature extraction act as a vital part in the accomplishment of watermarking schemes. Effective feature signifiers must continue steady even when images experience numerous manipulations. Among the existing methods, Pseudo-Zernike Moments have grown noteworthy consideration due to their mathematical belongings and sturdiness.

Pseudo-Zernike Moments are orthogonal image signifiers proficient to representing image features with negligible redundancy. Their rotation-invariant property empowers trustworthy image examination even at what time the image alignment changes. Moreover, PZM descriptors establish robust resistance to noise and firmness artifacts, creating them highly appropriate for digital watermarking submissions.

Numerous studies have exposed that PZM-enable watermarking schemes attain excellent watermark finding rates under stimulating circumstances. Meanwhile the instants are derivative from universal image features, they deliver a steady representation that leftovers consistent contempt to moderate distortions. To complement the universal representation providing by PZM, SURF is combined into the outline. The SURF is a characteristics detection and description method designed for speedy and precise recognition of the local key facts. It competently notices image structures that remain invariant to scale and rotational deviations. This competence permits the watermarking scheme to recognize corresponding areas even afterward geometric alterations.

The amalgamation of PZM and SURF generates a hybrid characteristics withdrawal model that profits from both universal and resident image depictions. Whereas PZM confirms robustness in contradiction of rotational alterations, SURF assists in recognizing invariant characteristics locations for precise watermark harmonization and retrieval.

## 3. GEOMETRIC TRANSFORMATION MODELLING AND SYNCHRONIZATION RECOVERY

Geometric attacks characterize one of the furthermost grim challenges in digital watermarking. Unlike the signal-processing attacks, geometric alterations change the spatial association among image pixels, and producing synchronization loss among the extraction algorithm and embedded watermark.

Affine transformations incorporate a comprehensive class of geometric alterations that comprise rotation, scaling, translation and shearing. These alterations are often applied moreover purposely by attackers or inadvertently throughout image processing processes.

The conventional watermarking methods frequently fail when exposed to affine distortions for the reason that they depend on on fixed spatial coordinates intended for watermark extraction. In contrast, invariant feature-based methods might recognize stable image features irrespective of geometric deviations.

In the anticipated framework, affine transformation modelling is active to guesstimate distortion limits and reestablish synchronization. PZM descriptors deliver rotational invariance, whereas SURF main points backing in placement of corresponding image areas. Together, these methods permit precise approximation of geometric transformations and simplify trustworthy watermark extraction.

The capability to recuperate synchronization meaningfully improves scheme resilience against solo and manifold geometric attacks. As a consequence, the outline might successfully regain watermark data even when images practice substantial geometric alterations.

## 4. MULTI-SHARE VISUAL CRYPTOGRAPHY FOR SECURE WATERMARK DISTRIBUTION

Visual Cryptography is an influential security procedure that defends visual information by separating it into manifold shares. Every share seems as random noise and does not disclose any expressive information when observed independently. The unique image might only be renovated when entire essential shares are united.

In this context, a four-share Visual Cryptography Scheme is used to improve watermark safety. The watermark is decayed into four self-regulating shares, every stored or conveyed separately. Since no separate share encompasses adequate information to rebuild the watermark, unauthorized users might not retrieve the protected data.

The usage of multiple shares delivers some security benefits. Foremost, it removes the risk related with storing the comprehensive watermark in a solo position. Additionally, it confirms that an attacker must get all shares to restructure the actual watermark. Third, its proposals additional guard against seizure and unauthorized revelation.

Once integrated with watermarking methods, Visual Cryptography delivers an additional layer of guard beyond traditional embedding procedures. Even when an attacker positively extracts fractional watermark information, rebuilding remains unbearable deprived of access to the entire cryptographic shares.

Subsequently, multi-share Visual Cryptography knowingly reinforces the safety and consistency of watermark-based authentication schemes.

## 5. HYBRID STRATEGY FOR COUNTERING COMBINED RST ATTACKS

Contemporary attackers frequently pay mixtures of geometric transformations to overthrow watermarking structures. Concurrent application of rotation, scaling and translation generates a compound attack situation identified as a collective or two-fold RST attack. Such attacks are mainly challenging for the reason that they present unembellished synchronization errors.

To resolve this subject, the projected framework accepts a hybrid watermarking policy that mixes multiple harmonizing methods. PZM signifiers deliver rotational invariance and steady image illustration, whereas SURF main points recognize conforming image regions in spite of scaling and translation. Affine transformation approximation more assists in recompensing for geometric distortions.

The watermark is entrenched inside invariant regions recognized through characteristics investigation. Throughout extraction, the similar features are cast-off to locate and line up the watermark-containing areas. This method reduces synchronization errors and expands extraction correctness.

Experimental conclusions stated in connected studies designate that hybrid feature-enabled approaches outperform conventional watermarking methods when endangered to complex geometric attacks. The mixture of worldwide descriptors, resident features and geometric rectification procedures consequences in significantly advanced watermark recovery degree and sturdier confrontation to intentional image operations.

## 6. DUAL-LAYER SECURITY USING QR CODES AND VISUAL CRYPTOGRAPHY

Security improvement is a key objective of privacy-preserving watermarking schemes. To accomplish this objective, the projected framework familiarizes a dual-layer safety structure that syndicates QR code expertise with Visual Cryptography.

### 6.1 QR Code-Based Information Protection

Quick Response (QR) codes have developed extensively cast-off due to their capability to store huge amounts of information proficiently. Their built-in error improvement ability confirms reliable decoding even when shares of the code are spoiled or slanted. In the anticipated outline, subtle watermark information is initially encoded in side QR code. This encoded illustration offers numerous benefits, with high storage ability, fast decoding and sturdiness in contradiction of image deprivation. Moreover, QR codes might securely store validation data, encryption keys and possession information. The usage of QR codes improves both security and reliability, confirming that watermark information relics recoverable under opposing situations.

### 6.2 Integration with Visual Cryptography

To added reinforce protection, the produced QR code is managed by utilising the four-share Visual Cryptography Scheme. This makes a two-level safety structure. The first stage contains of QR code encrypting, which converts watermark information in a machine-readable set-up. The second stage spread over Visual Cryptography to split the encrypted information into manifold shares. This layered safety method confirms that conciliatory one protection procedures does not expose the fundamental information. An attacker would requirement to overawed both QR code safety and Visual Cryptography fortification concurrently, meaningfully growing the trouble of unlawful access.

## 7. EVALUATION CRITERIA FOR CRYPTOGRAPHIC PERFORMANCE

The efficiency of a privacy-preserving watermarking structure be contingent not only on watermark sturdiness but also on the forte of its cryptographical elements. Numerous presentation metrics are usually cast-off to assess cryptographic algorithms.

### 7.1 Security Effectiveness

Security efficiency mentions to the capability of an algorithm to struggle brute-force attacks, the statistical assessment and cryptanalytic approaches. Robust algorithms uphold privacy and integrity even under antagonistic circumstances.

### 7.2 Processing Complexity

Computational complexity assesses the resources and accomplishment time needed for encoding and decoding actions. Well-organized algorithms are vital for practical disposition, mainly in large-scale multimedia submissions.

### 7.3 Data Processing Efficiency

Throughput assesses the size of information processed within an explicit time intermission. High amount is essential for real-time multimedia schemes that manage big amounts of digital content.

### 7.4 Sensitivity to Secret Keys

A safe cryptographic algorithm should display robust key understanding. Even a minor alteration in the encoding key should create a noteworthy diverse encoded output, thus preventing unlawful key approximation.
Together, these assessment criteria deliver a all-inclusive assessment of cryptographic performance and help control the appropriateness of safety algorithms for multimedia safety schemes.

## 8. POTENTIAL APPLICATION DOMAINS

The anticipated watermarking and privacy-preserving outline might be hired in many application domains necessitating secure multimedia administration. These comprise copyright safety for digital images, protected image sharing platforms, medical image verification, military communication schemes, cloud-enabled multimedia stowage and social media data authentication.
The blend of watermarking, encoding, QR codes and Visual Cryptography empowers trustworthy possession authentication and protected information exchange crossways of diverse atmospheres.

## 9. EXISTING CHALLENGES AND FUTURE PERSPECTIVES

In spite of its frequent benefits, the anticipated outline faces numerous applied challenges. The combination of manifold approaches upsurges computational difficulty and might necessitate additional processing resources. Moreover, harmonization amid Visual Cryptography shares might converted stimulating in distributed atmospheres. Upcoming

research should emphasis on dipping computational upstairs through optimization methods. Artificial Intelligence and Machine Learning algorithms might be employed to expand feature selection and attack recognition. Real-time employment for video watermarking submissions characterizes another capable research track. Moreover, blockchain expertise might be combined with watermarking schemes to generate decentralized ownership confirmation procedures. Such incorporation could added reinforce traceability, transparency and safety in multimedia fortification applications.

## 10. CONCLUSION

The article depicts privacy-preserving watermarking outline that syndicates Pseudo-Zernike Moments, SURF feature / characteristics extraction, affine transformation modelling, QR code encrypting and a four-share Visual Cryptography Scheme. The anticipated article resolves the inadequacies of conventional watermarking schemes by giving strong resistance in contradiction of rotation, scaling, and translation attacks whereas concurrently improving security vis multiple layers of fortification. The incorporation of worldwide and resident feature forms expands synchronization and watermark recovery, while QR codes and Visual Cryptography deliver safe information distribution and storage. Furthermore, cryptographic assessment focuses the significance of balancing safety, computational competence, and sturdiness.

## REFERENCES:

1. Sheshang D. Degadwala, Sanjay Gaur (2017): Privacy Preserving System Using Pseudo Zernike moment with SURF & Affine Transformation on RST Attacks, International Journal of Computer Science and Information Security (IJCSIS), 15(4), 147-152.

2. S. D. Degadwala and S. Gaur (2017): Two-way privacy preserving system using combine approach: QR-code & VCS,2017 Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, India, 2017, pp. 1-5, doi: 10.1109/IPACT.2017.8245120.

3. Degadwala, S.D., Gaur, S. (2018): 4-Share VCS Based Image Watermarking for Dual RST Attacks. Computational Vision and Bio Inspired Computing, Lecture Notes in Computational Vision and Biomechanics, vol 28. Springer, Cham. https://doi.org/10.1007/978-3-319-71767-8_77

4. Sheikh, M.F.A., Gaur, S., Desai, H., Sharma, S.K. (2019): A Study on Performance Evaluation of Cryptographic Algorithm. Emerging Trends in Expert Applications and Security. Advances in Intelligent Systems and Computing, vol 841. Springer, Singapore. https://doi.org/10.1007/978-981-13-2285-3_44

5. S. D. Degadwala and S. Gaur (2016): A study of privacy preserving system based on progressive VCS and RST attacks, 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC), Jalgaon, India, 2016, pp. 138-142, doi: 10.1109/ICGTSPICC.2016.7955285.

6. Solanki, N., Khandelwal, S., Gaur, S., Gautam, D. (2019): A Comparative Analysis of Wavelet Families for Invisible Image Embedding, Emerging Trends in Expert Applications and Security. Advances in Intelligent Systems and Computing, vol 841. Springer, Singapore. https://doi.org/10.1007/978-981-13-2285-3_27

7. Gaur, S., Pandya, D.D., Sharma, M.K. (2020): Applied N F Interpolation Method for Recover Randomly Missing Values in Data Mining. In: Yang, XS., Sherratt, S., Dey, N., Joshi, A. (eds) Fourth International Congress on Information and Communication Technology. Advances in Intelligent Systems and Computing, vol 1027. Springer, Singapore. https://doi.org/10.1007/978-981-32-9343-4_38.

8. Sheshang D. Degadwala and Sanjay Gaur (2017) An Efficient Image Watermarking for Combination of RST Attacks, International Journal of Computer Applications (0975 – 8887) Volume 170 – No.5, July 2017.

9. Sheshang Degadwala, Sanjay Chaudhary and Sanjay Gaur (2017), An Efficient ROI based Medical Image Watermarking on Non-Symmetric Rotation Attacks, IJSRSET, vol-3, no-8, 900-905.