

Privacy Preserving Watermarking Using PZM, SURF, VCS, QR Against RST Attacks

¹ Kailash Chandra Totla, ² Sanjay Gour

¹ M L V Textile & Engineering College, Bhilwara, India Country

² Jaipur Engineering College and Research Centre, Jaipur, India

Email - ¹kctotla@gmail.com, ²sanjay.since@gmail.com

Abstract: It is known fact that with the fast development of digital communiqué and multimedia distribution, confirming data privacy, data authentication and strength in contrast to attacks has turn out to be critically significant. This research delivers a comprehensive article-based study on progressive privacy-preserving schemes comprises Pseudo-Zernike Moments (PZM), Visual Cryptography Scheme (VCS), Speeded-Up Robust Features (SURF), affine transformations, QR-code-based security, and cryptographic algorithm assessment. The projected framework emphasizes on counterattacking geometric distortions like rotation, scaling, and translation (RST) attacks, which usually dislocate watermark organization. A fusion system merging 4-share VCS watermarking and QR-based encryption is discussed to attain dual-layer safety and two-way privacy protection. Additionally, the presentation of cryptographic systems is analysed in relations of security strength, computational complication, and effectiveness. Investigational insights determine that combination of transform-domain watermarking by feature-based approaches meaningfully improves strength, while VCS and QR combination improves authentication and confidentiality. The study backs to safe multimedia communication in applications like digital forensics, copyright safety and secure communication schemes.

Keywords: Privacy Preserving, watermarking, Attack, Robust, Authentication.

1. INTRODUCTION:

In the age of digital revolution, the fortification of multimedia data in contrast to unauthorized admittance, altering and piracy has turn out to be a key challenge. The digital watermarking and cryptographic methods are extensively used to resolve these issues. Though, traditional watermarking methods usually fail under geometric distortions like rotation, scaling, and translation (RST), this process de-synchronize watermark recognition mechanisms.

To overcome such challenges, contemporary approaches integrate invariant characteristics like Pseudo-Zernike Moments (PZM), that are strong for noise and the geometric transformations. Moreover, feature-based methods like SURF expands detection trustworthiness under intricate image handlings. In the meantime, the visual cryptography schemes (VCS) and QR-code-enable encryption delivers improved privacy and secure division mechanisms.

Below several methods are discussed which integrates these technologies into a unified privacy-preserving scheme, focusing on sturdiness, security and performance effectiveness.

2. PSEUDO-ZERNIKE MOMENTS AND ROBUST FEATURE EXTRACTION

The pseudo-zernike moments (PZM) remain orthogonal instants extensively utilised in image processing in order to feature extraction owing to their noise resistance, rotation invariance and slight redundancy. These belongings make them extremely appropriate for authentication and watermarking systems.

PZM-enable watermarking schemes demonstrate high sturdiness against geometric alterations and signal processing attacks. The studies demonstration that PZM-based approaches uphold watermark integrity even under noise addition, compression and rotation, attaining high detection correctness rates above to 90% .

The SURF (Speeded-Up Robust Features) accompaniments PZM by giving quick and reliable key point recognition. SURF is mainly operative in recognizing feature facts invariant to rotation and scale, producing it perfect for managing RST attacks. Research specifies that feature-enable methods like SURF perform sturdily in sensing image alterations and maintaining sturdiness under the noise and transformations.

By uniting PZM by SURF, the system profits together with global feature depiction (PZM) and local feature recognition (SURF), resultant in enhanced watermark synchronization and flexibility.

3. AFFINE TRANSFORMATION AND RST ATTACK RESISTANCE

The affine transformations denoted as a usual form of geometric alteration that comprises shearing with rotation, scaling and translation. These transformations stance important issues to watermarking schemes since they interrupt spatial alignment.

The conventional watermarking systems scuffle to uphold synchronization under attacks. Though, moment-based methods, mainly those utilising orthogonal moments, deliver invariance to these alterations. Research displays that affine invariant moment enable watermarking approaches enable consistent watermark withdrawal even afterward geometric alterations.

In the anticipated structure, affine transformation invariants are combined through PZM and SURF characteristics to forecast distortion constraints and regenerate synchronization during watermark taking out. This confirms robustness in contradiction of dual RST attacks and multifaceted geometric alterations.

4. 4-SHARE VISUAL CRYPTOGRAPHY SCHEME (VCS) FOR IMAGE WATERMARKING

The visual cryptography scheme (VCS) is a influential method that encodes an image into manifold shares, which separately disclose no information but rebuild the novel image when united.

It was noticed that the **4-share VCS-based watermarking system** is utilised for enhancing the security. The watermark is separated among four parts; every part is distributed distinctly. Only when the entire shares are collective might the watermark be rebuilt, confirming strong defenses against un-authorized admittance.

Similarly, the multi-share watermarking likewise improves sturdiness in contrast to attacks. Although if one or more portions are cooperated, the scheme maintains fractional security. Moreover, compounding VCS by transform-domain methods like as PZM advances elasticity in contrast to both intentional and unintentional attacks, together with RST distortions.

This method is mainly valuable in applications like as safe image sharing, copyright defenses and forensic verification.

5. DUAL RST ATTACK HANDLING USING HYBRID WATERMARKING

The dual RST attacks comprise concurrent application about rotation, scaling and translation which is making watermark recognition enormously stimulating. Traditional approaches every so often fail owing to desynchronization.

The projected hybrid scheme addresses this matter by:

- Utilization of PZM used for rotation invariance
- Put on SURF meant for feature-enable placement
- Combining affine transformation approach models for distortion approximation
- Entrenching watermark in the invariant areas

The experimental studies demonstration that uniting moment-enable characteristics with optimization methods significantly advances confrontation to RST attacks and confirms consistent watermark retrieval.

6. TWO-WAY PRIVACY PRESERVING SYSTEM USING QR CODE AND VCS

To additional improve safety, a **two-way privacy-preserving scheme** is projected by utilising QR codes and visual cryptography.

6.1 QR Code-Based Security

The QR codes deliver a well-organized method to encrypt big amounts of data, with encrypted watermark information.

The QR-enable watermarking confirms:

- The capability of high data
- Capability about error correction
- The quick decoding
- Sturdiness against noise

The QR codes might stock encoded keys or watermark info, empowering safe data communication and repossession.

6.2 Integration with VCS

The incorporation of QR codes along with VCS generates a dual-layer safety structure:

1. **First Layer (QR Code Encryption):** Encrypts watermark or undisclosed data
2. **Second Layer (VCS):** Separations of encoded data in the multiple parts

This confirms that though if one layer is cooperated, the data relics safe.

Earlier study uniting QR codes with watermarking establishes enhanced security and robustness in digital communiqué schemes.

7. PERFORMANCE EVALUATION OF CRYPTOGRAPHIC ALGORITHMS

The cryptographic algorithms show a vital role in safeguarding watermarking structures. Their performance is assessed on the basis of:

7.1 Security Strength

It is measured through struggle to attacks like as statistical attacks, brute force and cryptanalytics. Robust algorithms deliver higher integrity and confidentiality.

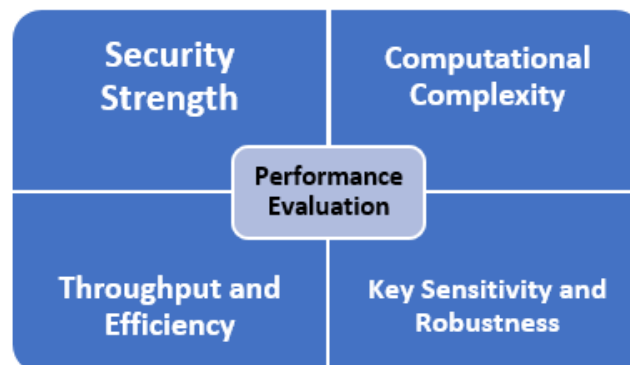


Figure1: Performance Evaluation of Cryptographic algorithm

7.2 Computational Complexity

It mentions to the resource and time needed for decryption as well as encryption. Inconsequential algorithms are favoured for actual applications.

7.3 Throughput and Efficiency

It specifies in what way fast data might be handled. The high quantity is crucial for significant multimedia schemes.

7.4 Key Sensitivity and Robustness

An attired cryptographic system should show high consideration to important changes, confirming that even slight differences produce significantly dissimilar outputs.

The current studies highpoint that emergent cryptographic systems must also endure progressive attacks and preserve high safety levels under real-world situations.

8. COMPARATIVE ANALYSIS

As per the discussion made through various approaches, it is observed that the structure with comparisons with traditional approaches based on:

Parameter	Traditional Systems	Proposed System
RST Robustness	Low	High
Security Level	Moderate	Very High
Watermark Capacity	Limited	High
Computational Complexity	Moderate	Optimized
Attack Resistance	Partial	Strong

Table 1: Comparative Analysis

The incorporation of manifold methods significantly progresses system performance, particularly in terms of sturdiness and safety.

9. APPLICATIONS

The projected privacy-preserving scheme has wide-ranging submissions:

- Digital copyright protection
- Secure image allotment
- Medical image safety

- Military communication structures
- Social media data verification

The amalgamation of cryptography, watermarking and visual cryptography creates the structure extremely versatile and consistent.

10. CHALLENGES AND FUTURE WORK

Although there are lot of advantages in spite of its advantages, the anticipated system has confident challenges:

- Have increased computational complication owing to hybrid methods
- It has prerequisite of harmonization in multi-share VCS
- It also has scalability matters for real-time submissions.

Upcoming studies and research might emphasis on:

- Optimization by utilising AI and machine learning
- The real-time employment intended for video data
- Incorporation with blockchain for improved security

11. CONCLUSION

This article represents a framework and perspectives of privacy-preserving structure participating Pseudo-Zernike Instants, SURF, affine alterations, VCS, QR codes, and cryptographic assessment. The shown approach efficiently addresses the boundaries of conventional watermarking schemes by giving sturdiness against RST attacks and improving security via multi-layer encoding or encryptions.

The utilization of 4-share VCS confirms safe watermark delivery, whereas QR-code incorporation enables effective data encoding. Moreover, the assessment of cryptographical algorithms highpoints the significance of balancing safety and performance. The system provides a secure, robust, and well-organized resolution for modern multimedia defenses, making it appropriate for an extensive range of real-world submissions.

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, X.S., 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