IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 10, Issue.6, June 2022 E-ISSN: 2347-2693

Invisible Watermark based Image Authentication System with 5/3 Integer Wavelet Transform

Bibek Ranjan Ghosh[1]*, Siddhartha Banerjee[2], Deepro Sarkar[3]

[1,2,3]Department of Computer Science, Ramakrishna Mission Residential College, Narendrapur, Kolkata-700103

**Corresponding author: bibekghosh2019@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v10i6.2226 | Available online at: www.ijcseonline.org

Received: 20/May/2022, Accepted: 09/Jun/2022, Published: 30/Jun/2022

Abstract- The authentication techniques deals with the originality of an object. It may be image, text, audio etc. Image authentication widely use watermarking techniques both in spatial and transform domain, especially discrete wavelet based techniques are preferred for features like multilevel analysis and lossless reconstruction. Again, integer wavelets has added advantage of generating only integer coefficients which further make computation simpler and faster. This work initially used forward 5/3 integer wavelet transform (IWT) on cover image to generate sub bands. A watermark image is taken and its SHA256 hash code is generated. The watermark and hash code are embedded in two different sub bands using dynamic random position map and the sub bands are inverse 5/3 IWT transformed to generate stego image. During extraction, the opposite process is adopted and the hash code of extracted watermark is computed and compared with original hash code for verification of authenticity. The experimental observation of the proposed method revealed around 61.5dB peak signal to noise ratio (PSNR), near zero mean square error (MSE) and very high structural similarity index measure (SSIM) with 8448 bit payload and PSNR 55 dB with 33024 bits of payload.

Keywords: Watermarking, Lifting Scheme, IWT, Randomization, Authentication.

I. INTRODUCTION

The problem of authentication of documents in various forms e.g. text, audio, image etc is of practical importance in government organization and corporate houses to avoid the problem of impersonation and temper less distribution. Unauthenticated materials may lead to situations of legal action. So over the period many techniques were devised for authentication including watermarking.[1] Watermark is a small digital information visible/invisible is combined with original object. The originality of the object can be verified by extracting the watermark at the receiver end. In watermarking based image authentication the embedding can be done directly on the pixel domain or in the coefficients of the frequency domain of the input cover image.[2][3] The transform domain techniques have the advantage of resistance against external tampering attacks. Discrete wavelet based techniques have further advantage of multi-resolution analysis of cover image providing ample embedding options, wide array of wavelets like Haar, Daubechies, Morlet etc.[4][5][6] The wavelet transform produces one average sub-band LL and three detailed sub-band Hl, HH and LH in forward transform, whereas detailed bands are more suitable embedding as they produce high frequency components where distortion due to embedding would be lesser.[7] The main problem is high frequency transform coefficients are real numbers and need to be modified to hold secret data. But as they are real numbers during extraction so it need complex computation to recover the secret data and often gives error. Integer wavelet transform (IWT) solves this problem by generating only integer coefficients even in high frequency bands. Hence, embedding and extracting in high frequency bands take less computation time, produce high quality images and ensure recoverability. [5]Various IWT based methods are there but lifting scheme based integer wavelets as proposed by Swelden are efficient.[4][8] All transform mentioned by Swelden used linear phase Finite Impulse Response(LP-FIR) bank of filters. A single filter bank consists of an analysis and synthesis filters. The analysis filters consists of high and low pass filters with down sampling producing average and detail components whereas synthesis filters up samples them and combine them with filters producing original signal. These transforms are named as y/z notation where analysis filter has y low pass and z high pass filters. Some of them are Haar, 5/3, 9/7-M,2/6,13/7-T etc. [9]This work used 5/3 lifting scheme based IWT method to embed watermark and hash code. The rest of the sections are organized as follows. The Section-II studies related work, Section-III discuss proposed method, Section-IV depicts experimental results, analysis and comparison and finally Section-V concludes the work.

II. RELATED WORK

This section deals with the various works that can be found in the literature.

S.Fazli et al. presented a new method based on DCT,DWT and SVD which reduced geometric attack.[10] The cover is first partitioned into four parts and watermark is embedded in each of them leading to cropping attack resistance. Other attacks like rotation, translation are avoided using corner detection. Binary image and bit sequence are used as watermark. PSNR achieved 56.899dB for payload 2048bits having 0.0078bpb. Y.He et al. method used YUV color model.[11] DWT is applied for Y component. The high frequency HH band is splitted into 4x4 blocks and each block followed by DCT and SVD. Arnold transform is used on watermark and encoded in the ∑ components of SVD. PSNR reported is 48.14 dB for scale factor=1.2 with 64x64 binary watermark. The performance against gamma correction, JPEG compression etc found to be good. S.Islam et al. presented a IWT scheme based on lifting scheme using 3 levels, with HL coefficient use randomization and were splitted by 2x2 blocks.[12] Encrypted watermark bits were used for each block. PSNR reported was 43.88dB with 512 bit watermark. A.A.Khaleel et al. used color channels of cover image in embedding.[13] Arnold transform was applied on watermark and DCT applied next with division into blocks. DWT of of rgb channel were used to embed each block. Attacks like rotation, JPEG compression etc.were tested. Average PSNR found was 48 dB. R.Liu. et al presented a SVD based method. [14] The cover is decomposed into singular matrices U , V and diagonal matrix S. Water mark W is combined with S with a strength factor i.e. S+aW and SVD is performed on it to get three matrices. Again constituents are combined to get watermarked image. Random matrix are chosen as watermark. PSNR reported is 53.83dB for watermark size 8192 bits for capacity 0.0315 bpb. S.Kumar et al. presented an algorithm using DWT operation on Y component of YCbCr color channel. The HH band is divided by 64 blocks. [15] The highest entropy block is used for alpha embedding of watermark. PSNR found was 51.61 dB. O.Kwon et al. proposed a watermarking method for forgery detection in JPEG images using DCT transform and resist collage attack.[16] The cover was divided into many block group and watermark was generated using adjacent block group and embedded in them. Average PSNR observed up to 45 dB around 0.15 bpb. M.J.Barani et al. proposed a 3D quantum map based method which provide long-key space.[17] A new permutation is used on 2x2 blocks followed by SVD of blocks. U matrix is encrypted with chaotic map. IWT for embedding after authentication code is generated. MSRA, Corel, SIPI & KODAK dataset used and max PSNR reported 45.11 dB for 1.28 bpb.

III. METHODOLOGY

The proposed work first execute forward 5/3 integer wavelet transform on the grayscale cover image CVR and produces HL, LH and HH images as detailed sub-band along with approximate sub-band image LL, each sub-band image is half of CVR.[18] Another auxiliary watermark image WA is applied secure hash algorithm SHA256 to produce 256 bit hash code WAHASH which will act as authentication information.[19] Subsequently a randomization algorithm is used to find embedding location positions within sub-band HH and HL as sequences HHMAP and HLMAP respectively. WA is encoded in 8-bit binary is embedded within HH following HHMAP with k-bit (k<=8) per pixel LSB substitution. Similarly, WAHASH is embedded within HL following HLMAP. All four sub bands are then operated using 5/3 inverse transformation to construct stego image STG. At the receiver end STG first forward transformed using 5/3 IWT to produce HL, LH, HH and LL. The watermark image WA' is recovered from HH using HHMAP and hash value WAHASH' is recovered from HL using HLMAP. New SHA256 is computed from WA’ as NWAHSAH. Authentication is confirmed if WAHASH and NWAHASH are identical. The embedding and authentication steps are shown in Figure-1 and Figure-2 respectively. The subsections clarifies the essential algorithms.

A. *WAHASH Generation*

Perform row major conversion of grayscale WA of size PXQ into VEC of size P*Q. Concatenate the 8-bit encoding of elements of VEC into string WMSG. With UTF-8 encoding of WMSG, compute SHA-256 on WMSG generate hexadecimal hash code WAHASH having 64 elements and finally 256 bit.

B. Dynamic Embedding Position Map Generation

This algorithm has a seed value SD set as the sub-band (HH/HL) dimension selected for embedding. Set vector V={0, 1, 2…, (SD-1)}. Then, find a POS such that POS ϵ V, POS>2 and (POS, SD) satisfies co-primality. Initially, embedding position map MAP=φ. Then generate a random integer Next from set V. Append Next to MAP and set First=Next. Now repeatedly compute Next= (Next+ POS) Mod SD and append Next to MAP until First and Next are equal.

C. Forward 5/3 IWT

The one dimensional forward integer 5/3 transform of a one dimensional digital signal X with 2K elements into average A and detailed D sub bands is achieved Equation-(1),

$$\left.\begin{aligned} D[n] &= X[2n+1] - \left\lfloor \frac{1}{2}(X[2(n+1)] + X[2n]) \right\rfloor \\ A[n] &= X[2n] + \left\lfloor \frac{1}{4}(D[n] + D[n-1]) + \frac{1}{2} \right\rfloor \end{aligned}\right\} \quad (1)$$

for n=0, 1, 2, .., (K-1) where X[2n] and X[2n+1] represents even and odd signal elements in X. To forward transform a 2D image of size MXN, first convert all rows using Equation-(1). After that apply Equation-(1) to all columns yielded in previous step and apply equal split of four to generate HL, LL, LH and HH sub-bands each of size M/2XN/2 in four quadrants respectively.

D. Inverse 5/3 IWT

The one dimensional inverse 5/3 transform for signal reconstruction from average and detailed component A and D is governed by Equation-(2).

$$\left.\begin{aligned} X[2n] &= A[n] - \left\lfloor \frac{1}{4}(D[n] + D[n-1]) + \frac{1}{2} \right\rfloor \\ X[2n+1] &= D[n] + \left\lfloor \frac{1}{2}(X[2(n+1)] + X[2n]) \right\rfloor \end{aligned}\right\} \quad (2),$$

for n=0, 1, 2,., (K-1) to regenerate original signal of length 2K. To apply inverse transform in 2D image the input HL, LL, LH and HH are combined in an image of size MxN placed as four quadrants of it. Then apply Equation-(2) in all columns of it and subsequently apply Equation-(2) for all rows resulting from previous step to regenerate original 2D image.

IV. RESULTS AND DISCUSSION

A. *Result*

Several benchmark grayscale images of size 512x512 of the USC-SIPI database are employed as cover for the experiment. The resized images of same database of dimension 32x32 or 64x64 act as watermark. The metrics used to measure experimental performance are SSIM, PSNR and MSE computed form cover and stego images.[20] The Equation-(3) shows the expressions for SSIM, PSNR and MSE calculated between grayscale cover image (CVR) and stego image (STG) of size MxN.

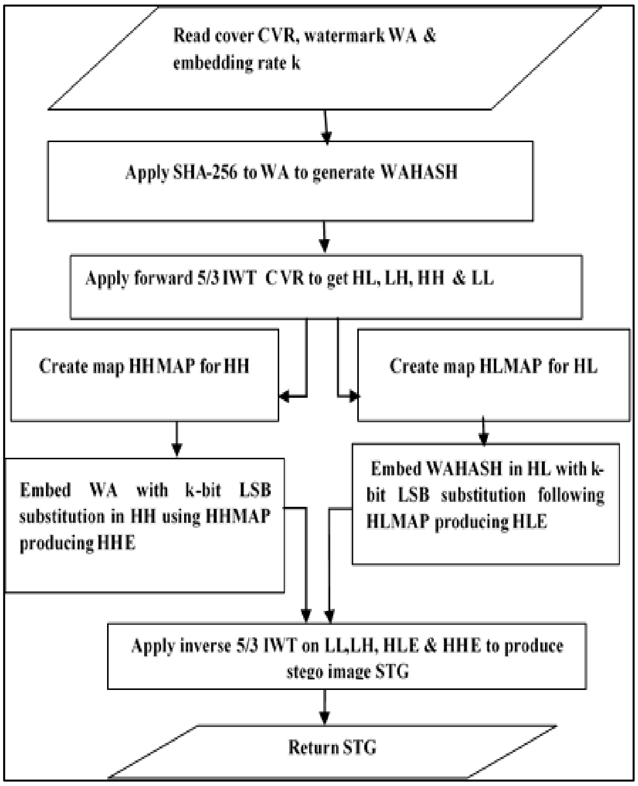

Figure-1: Proposed Embedding Flowchart

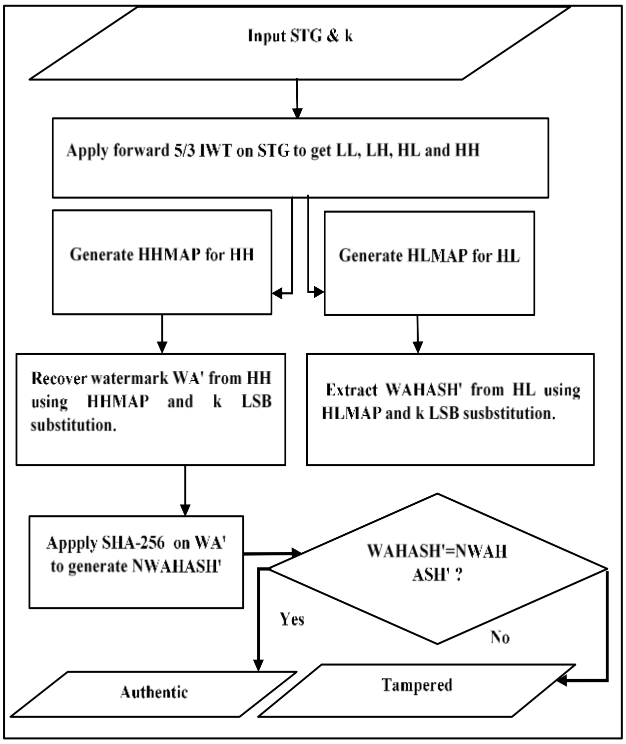

Figure-2: Proposed Extraction Flowchart

$$\left.\begin{aligned} MSE &= \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[CVR(i,j) - STG(i,j)] \\ PSNR &= 20\log\frac{255}{\sqrt{MSE}} \\ SSIM &= \frac{[2\mu(CVR)\mu(STG) + c1]*[2\sigma(CVR,STG) + c2]}{[\mu(CVR)^2 + \mu(STG)^2 + +c1]*[\sigma(CVR)^2 + \sigma(STG)^2 + c2]} \end{aligned}\right\} \quad (3)$$

, where μ and σ are mean and standard deviations whereas c1 and c2 are constants. [17] Table-1 show the performance of the proposed method for different covers in SIPI dataset for embedding rate k=2 and watermark size 32x32 and 64x64. A sample output is shown in Figure-3.

Figure-3: a) Cover b) Watermark c) Stego d) Recovered watermark

B. *Analysis of the Result*

The results show that the proposed algorithm can successfully recover the watermark in 100% cases without any deterioration and authenticity is found in all the cases. The visual quality of the stego images are quite good as the PSNR values ranges from 54dB to 61dB in all the cases whereas the base requirement is 30dB.MSE is close to zero signifies negligible distortion due to embedding and SSIM are near to one consolidates the superiority over many similar techniques. The original and extracted watermark are further verified and found SSIM=1 and PSNR=infinity which exhibits perfect watermark recovery.

Table-1: Performance of the proposed method for embedding rate k=2

Cover Image	Watermark 32x32			Watermark 64x64		
	MSE	***PSNR***	***SSIM***	***MSE***	***PSNR***	***SSIM***
Airport	0.0116	67.4739	0.9999	0.0453	61.5681	0.0996
House	0.0571	60.5625	0.9994	0.2285	54.5416	0.9975
Jetplane	0.0481	61.3135	0.9994	0.1845	55.4715	0.9982
Lake	0.0464	61.4615	0.9998	0.1802	55.5726	0.9990
Lena	0.0466	61.4494	0.9995	0.1788	55.6067	0.9986
Mandril	0.0517	60.9955	0.9997	0.2019	55.0798	0.9993
Pepper	0.0459	61.5172	0.9997	0.1813	55.5479	0.9987
Pirate	0.0471	61.3964	0.9997	0.1793	55.5952	0.9990
Plane	0.0117	67.454	0.9998	0.0458	61.522	0.9995
Tank	0.0456	61.5367	0.9998	0.1848	55.4634	0.9994

C. Comparison of Performance

Table-2: Comparison of performance with standard methods

Method	Cover Size	Technique	PSNR (dB)	Water mark (Bits)	Bits per Byte
Liu et al. [14]	512x512	SVD	53.83	8192	0.0315
Fazli S. et al. [10]	512x512	DWT, DCT & SVD	56.899	2048	0.0078
He Y. et al. [11]	512x512x3	DWT,DCT and SVD	48.14	8192	0.0104
Islam M. et al. [12]	512x512	LWT & ANN	43.88	512	0.0019
Khaleel et al [13]	1024x1024x3	DCT & DWT	48	73728	0.023
Proposed Method (k=2)	512x512	5/3 IWT	61.5	8448	0.032
Proposed Method (k=2)	512x512	5/3 IWT	54	33024	0.126

The results are further compared with similar DWT and IWT based techniques on the basis of algorithms applied, watermark size, PSNR, Cover size and embedding capacity (bpb) and listed the observation in Table-2. We observe that the proposed method when tested with 8192 bit watermark along with hash of 256 (total: 8448 bits) gives PSNR=61.5 dB and bpb=0.032 which is better than [14], [11]. The proposed method show superiority with respect to all of them in terms of all the parameter chosen for comparison.

V. CONCLUSION AND FUTURE SCOPE

The significance of authentication using image is well established method as can be found from the literature. This work first studied various similar methods used for image authentication and focused was on DWT transform domain techniques. The application of integer wavelet for distortion less recovery as well as integer representation of transform coefficients make the computation simpler and faster. The two tier verification, dynamic random location map generation, high PSNR, near zero MSE and very high SSIM are the superiority of this algorithm which is further verified in Table-2. Hence its practicality in authentication application can be concluded. The future direction of research may be to apply other IWT based transform algorithms, multilevel decomposition and advanced embedding techniques like PVD, histogram shifting etc.

ACKNOWLEDGMENT

The authors thank the members of faculty and staff of the Department of Computer Science of the Ramakrishna Mission Residential College Narendrapur, Kolkata-700103, West Bengal, India for their immense support and assistance in carrying out this research work.

AUTHOR CONTRIBUTIONS

Every author have contributed to the work equally and constantly researching on the context by critically studying relevant works and implementation of the models used so far.

FUNDING STATEMENT

This work is not funded by any institute, agency or individual and authors take responsibility in this respect.

DECLARATION OF CONFLICT OF INTEREST

All authors hereby declare that they don't have any conflicting financial interests or other relationships that have appeared here which may influence this work.

REFERENCES

[1] B. Li, J. He, J. Huang, Y. Q. Shi, "*A Survey on Image Steganography and Steganalysis*", Journal of Information Hiding and Multimedia Signal Processing., Vol**. 2**, Issue.**2**, pp.**142-172**, **2011.**

[2] J. Kadhim, P. Premaratne, P. J. Vial,B. Halloran , "*Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research*", Neurocomputing, Vol.**335**,Issue.**1**, pp.**300-306,2019**

[3] J. Fridrich, M. Goljan, R. Du, "*Reliable Detection of LSB Steganography in Color and Grayscale Images*", In the Proceedings of the Workshop on Multimedia and Security: New Challenges, ACM, **New York**, pp. **27-30**, **2001.**

[4] A. R. Calderbank, I. Daubechies, W. Sweldens, B.L. Yeo, "*Wavelet Transforms that Map Integers to Integers*", Applied and Computational Harmonic Analysis,Vol.**5**,Issue.**3**,pp.**332-369**, **1998.**

[5] N. Muhammad, N. Bibi, Z. Mahmood,D.G. Kim, "*Blind Data Hiding Technique using the Fresnelet Transform*", SpringerPlus, Vol.**4**,Issue.**1**,pp.**1-15**, **2015.**

[6] H. Daren, L. Jiufen, H. Jiwu,L. Hongmei, "*A DWT-Based Image Watermarking Algorithm*", In IEEE International Conference on Multimedia and Expo 2001- ICME 2001, IEEE Computer Society, **Tokyo**, pp.**313-316**, **2001**.

[7] S. Subburam, S. Selvakumar,S. Geetha, "*High Performance Reversible Data Hiding Schemethrough Multilevel Histogram Modification in Lifting Integer Wavelet Transform*", Multimedia Tools and Applications. Vol.**77**,Issue.**6**,pp.**7071-7095**, **2018**.

[8] W. Sweldens, "*The Lifting Scheme: A Construction of Second Generation Wavelets*", SIAM journal on Mathematical Analysis, Vol.**29**,Issue.**2**,pp.**511-546**, **1998**.

[9] A. Shaik,V. Thanikaiselvan,"*Comparative Analysis of Integer Wavelet Transforms in Reversible Data Hiding Using Threshold Based Histogram Modification*",Journal of King

Saud University-Computer and Information Sciences, Vol.**33**, Issue.**7**,pp.**878-889**, **2021**.

[10] S. Fazli,M. Moeini,"*A Robust Image Watermarking Method Based on DWT, DCT, and SVD Using a New Technique for Correction of Main Geometric Attacks*",Optik Vol.**127**, Issue.**2**,pp. **964-972**, **2016**

[11] Y. He and Y. Hu., "*A Proposed Digital Image Watermarking Based on DWT-DCT-SVD*," in 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), **IEEE, Xian**,pp.**1214-1218,2018**.

[12] M. Islam, A. Roy and L. R. Hussain, "*Neural Network Based Robust Image Watermarking Technique in LWT Domain*", Journal of Intelligent & Fuzzy Systems, Vol. **34**,Issue.**3**, pp.**1691-1700**, **2018**.

[13] A. A. Khaleel ,O. Serkan,"*A Novel Hybrid DCT and DWT Based Robust Watermarking*", Multimedia Tools and Applications, Vol.**12**, Issue.**78**, pp.**17027-17049**, **2019**.

[14] R. Liu,T. Tan, "*An SVD-Based Watermarking Scheme for Protecting Rightful Ownership*", IEEE Transactions on Multimedia,Vol.**4**,No.**1**,pp.**121-128**, **2002.**

[15] S. Kumar,S. B. Kumar,"*DWT Based Color Image Watermarking using Maximum*", Multimedia Tools and Applications, Vol.**80**,Issue.**10**,pp.**15487-15510**, **2021**.

[16] O.J. Kwon, S. Choi,B. Lee,"*A Watermark-Based Scheme for Authenticating JPEG Image Integrity*", IEEE Access, Vol. **6**,Issue.**1**,pp. **46194-46205**, **2018**.

[17] M. J. Barani, M. Y. Valandar,P. Ayubi, "*A New Digital Image Tamper Detection Algorithm Based on Integer Wavelet Transform and Secured by Encrypted Authentication Sequence With 3D Quantum Map*",Optik-International Journal of Light and Electron Optics,Vol.**187**,Issue.**1**, pp.**205-222**, **2019.**

[18] M. D. Adams, F. Kossentini,R. K. Ward, "*Generalized S Transform*", IEEE Transactions on Signal Processing , Vol. **50**, Issue.**11**, pp.**2831-2842**, **2002**.

[19] I. Ahmad,A. S. Das,"*Hardware Implementation Analysis of SHA-256 and SHA-512 Algorithms on FPGAs*",Computers & Electrical Engineering,Vol.**31**,Issue.**6**,pp.**345-360**, **2005**.

[20] A. Pradhan, A. K. Sahu, G. Swain,K. R. Sekhar, "*Performance Evaluation Parameters of Image Steganography Techniques*", In 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), **IEEE, Banglore**, pp**.1-8**, **2016**.

AUTHORS PROFILE

Bibek Ranjan Ghosh (MCA), University of North Bengal, is actively teaching as Assistant Professor, in the Department of Computer Science (CS), Ramakrishna Mission Residential College, (RKMRC), Narendrapur Kolkata, India since 2008. He has published and presented many research articles in national and international journal and conferences including Scopus index journals. His research areas are computer vision, steganography &data science.

Dr. Siddhartha Banerjee, M.Tech from Calcutta University,Ph.D from Jadavpur University and currently working as an Assistant Professor & HOD in the Department Computer Science in the RKMRC Narendrapur, Kolkata-700103,since 2008. His research interests are digital image processing, VLSI, AI & cryptography. His publication include national and international journal & conferences of repute.

Deepro Sarkar is currently an under graduate student of the 6th semester, B.SC. Computer Science (Hons) in the Department of Computer Science of RKMRC Narendrapur, Kolkata-700103. West Bengal. His area of interest are image processing and computer vision

